

MANUEL DE L'UTILISATEUR

KASPERSKY ANTI-VIRUS 2010



Chers utilisateurs !

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce manuel vous sera utile et qu'il répondra à la majorité des questions.

La copie sous n'importe quelle forme et la diffusion, y compris la traduction, de n'importe quel document sont admises uniquement sur autorisation écrite de Kaspersky Lab.

Ce document et les illustrations qui l'accompagnent peuvent être utilisés uniquement à des fins personnelles, non commerciales et informatives.

Ce document peut être modifié sans un avertissement préalable. La version la plus récente de ce document est accessible sur le site de Kaspersky Lab à l'adresse <http://www.kaspersky.com/fr/docs>.

Kaspersky Lab ne pourra être tenu responsable du contenu, de la qualité, de l'actualité et de l'exactitude des textes utilisés dans ce manuel et dont les droits appartiennent à d'autres entités. La responsabilité de Kaspersky Lab en cas de dommages liés à l'utilisation de ces textes ne pourra pas non plus être engagée.

Ce manuel fait référence à des noms qui sont des marques déposées ou non. Elles appartiennent toutes à leur propriétaire respectif.

Copyright © Kaspersky Lab 1997 - 2009

<http://www.kaspersky.com/fr>
<http://support.kaspersky.com/fr>

Date d'édition : 22/05/09

TABLE DES MATIERES

INTRODUCTION	9
Distribution.....	9
Services pour les utilisateurs enregistrés.....	9
Configuration matérielle et logicielle requises	10
KASPERSKY ANTI-VIRUS 2010.....	11
Obtention d'informations sur l'application.....	11
Sources d'informations pour une aide autonome	11
Contacter le service Commercial	12
Contacter le service d'assistance technique	12
Discussion sur les logiciels de Kaspersky Lab dans le forum en ligne	13
NOUVEAUTES DE KASPERSKY ANTI-VIRUS 2010.....	14
CONCEPT DE LA PROTECTION DE VOTRE ORDINATEUR.....	15
Composants de la protection.....	15
Tâches de recherche d'éventuels virus.....	17
Mise à jour	17
Protection des données et de l'activité en ligne.....	18
Assistants et outils.....	18
Fonctions de service de l'application	18
INSTALLATION DE KASPERSKY ANTI-VIRUS SUR L'ORDINATEUR	20
Etape 1. Recherche d'une version plus récente de l'application.....	21
Etape 2. Vérification des configurations minimum requises pour l'installation	21
Etape 3. Sélection du type d'installation.....	22
Etape 4. Lecture du Contrat de licence.....	22
Etape 5. Règlement d'utilisation de Kaspersky Security Network.....	22
Etape 6. Sélection du répertoire d'installation	22
Etape 7. Sélection des composants de l'application à installer.....	23
Etape 8. Utilisation des paramètres de l'application conservés de l'installation antérieure.....	23
Etape 9. Recherche d'autres logiciels antivirus	24
Etape 10. Derniers préparatifs pour l'installation de l'application	24
Etape 11. Fin de la procédure d'installation	24
PREMIERE UTILISATION.....	25
Assistant de configuration de l'application.....	26
Etape 1. Activation de l'application.....	26
Activation de la version commerciale	27
Activation de la version d'évaluation	27
Fin de l'activation	27
Etape 2. Sélection du mode de protection	28
Etape 3. Configuration de la mise à jour de l'application	28
Etape 4. Restriction de l'accès à l'application	29
Etape 5. Sélection des menaces identifiées	29
Etape 6. Fin de l'Assistant	29
Mise à jour de l'application.....	29
Recherche de virus sur l'ordinateur	30
Recherche de vulnérabilités sur l'ordinateur.....	30

Administration de la licence.....	30
Abonnement pour le renouvellement automatique de la licence	31
Participation au Kaspersky Security Network.....	32
Administration de la sécurité	33
Etat de la protection.....	35
Suspension de la protection.....	35
INTERFACE DE L'APPLICATION	37
Icône dans la zone de notification	37
Menu contextuel	38
Fenêtre principale de Kaspersky Anti-Virus	39
Notifications	41
Fenêtre de configuration des paramètres de l'application.....	41
PROTECTION DU SYSTEME DE FICHIERS DE L'ORDINATEUR.....	42
Algorithme de fonctionnement du composant	43
Modification du niveau de protection des fichiers et de la mémoire	44
Modification de l'action à réaliser sur les objets identifiés	44
Constitution de la zone de protection.....	45
Utilisation de l'analyse heuristique.....	46
Optimisation de l'analyse	46
Analyse des fichiers composés	47
Analyse des objets composés de grande taille.....	47
Modification du mode d'analyse	48
Technologie d'analyse	48
Suspension du composant : programmation	49
Suspension du composant : composition de la liste des applications	50
Restauration des paramètres de protection par défaut	51
PROTECTION DU COURRIER.....	52
Algorithme de fonctionnement du composant	53
Modification du niveau de protection du courrier	53
Modification de l'action à réaliser sur les objets identifiés	54
Constitution de la zone de protection.....	55
Analyse du courrier dans Microsoft Office Outlook	55
Analyse du courrier dans The Bat!	56
Utilisation de l'analyse heuristique.....	56
Analyse des fichiers composés	57
Filtrage des pièces jointes.....	57
Restauration des paramètres de protection du courrier par défaut.....	58
PROTECTION DU TRAFIC INTERNET	59
Algorithme de fonctionnement du composant	60
Modification du niveau de protection du trafic HTTP.....	61
Modification de l'action à réaliser sur les objets identifiés	61
Constitution de la zone de protection.....	62
Sélection du type d'analyse.....	62
Module d'analyse des liens	63
Utilisation de l'analyse heuristique.....	64
Optimisation de l'analyse	64
Restauration des paramètres de protection Internet par défaut.....	65

PROTECTION DU TRAFIC DES MESSAGERIES INSTANTANÉES	66
Algorithme de fonctionnement du composant	67
Constitution de la zone de protection.....	67
Sélection de la méthode d'analyse	67
Utilisation de l'analyse heuristique.....	68
DEFENSE PROACTIVE.....	69
Utilisation de la liste des activités dangereuses.....	69
Modification d'une règle de contrôle de l'activité dangereuse.....	70
Constitution d'un groupe d'applications de confiance	71
Contrôle des comptes utilisateur système.....	71
ANALYSE DE L'ORDINATEUR.....	72
Recherche de virus.....	72
Lancement de l'analyse.....	74
Création de raccourcis pour le lancement d'une tâche	75
Composition de la liste des objets à analyser	75
Modification du niveau de protection	76
Modification de l'action à exécuter après la découverte d'une menace	77
Modification du type d'objets à analyser	77
Optimisation de l'analyse.....	78
Analyse des disques amovibles	78
Analyse des fichiers composés.....	79
Technologie d'analyse.....	80
Modification de la méthode d'analyse.....	80
Mode de lancement : programmation.....	81
Mode de lancement : configuration du compte utilisateur	81
Particularité du lancement programmé des tâches de l'analyse.....	82
Restauration des paramètres d'analyse par défaut	82
Recherche de vulnérabilités.....	82
Lancement de la recherche de vulnérabilités.....	83
Création de raccourcis pour le lancement d'une tâche	84
Composition de la liste des objets à analyser	84
Mode de lancement : programmation.....	85
Mode de lancement : configuration du compte utilisateur	85
MISE A JOUR.....	87
Lancement de la mise à jour	88
Annulation de la dernière mise à jour	89
Sélection de la source de mises à jour	89
Utilisation du serveur proxy.....	90
Paramètres régionaux	90
Actions exécutées après la mise à jour.....	91
Mise à jour depuis un répertoire local	91
Modification du mode de lancement de la tâche de mise à jour	92
Lancement de la mise à jour avec les privilèges d'un autre utilisateur	92
CONFIGURATION DES PARAMÈTRES DE L'APPLICATION.....	94
Protection.....	95
Activation / désactivation de la protection de l'ordinateur	95
Lancement de Kaspersky Anti-Virus au démarrage du système d'exploitation	96

Utilisation du mode de protection interactif	96
Restriction de l'accès à Kaspersky Anti-Virus	97
Antivirus Fichiers	97
Antivirus Courrier	98
Antivirus Internet	99
Antivirus IM ("Chat")	100
Défense Proactive	100
Analyse	101
Mise à jour	102
Paramètres	102
Autodéfense de Kaspersky Anti-Virus	102
Technologie de réparation des infections actives	103
Fonctionnement de Kaspersky Anti-Virus sur un ordinateur portable	103
Performances de l'ordinateur pendant l'exécution des tâches	104
Exportation/importation des paramètres de fonctionnement de Kaspersky Anti-Virus	104
Restauration des paramètres par défaut	105
Menaces et exclusions	105
Sélection des catégories de menaces identifiées	106
Sélection des applications de confiance	106
Règles d'exclusion	107
Réseau	109
Constitution de la liste des ports contrôlés	109
Analyse des connexions sécurisées	110
Analyse des connexions sécurisées dans Mozilla Firefox	111
Analyse des connexions sécurisées dans Opera	112
Paramètres du serveur proxy	112
Notifications	113
Désactivation de la sonorisation des notifications	114
Envoi des notifications à l'aide du courrier électronique	114
Rapports et Stockages	114
Ajout d'enregistrements relatifs aux événements dans le rapport	115
Purge des rapports	115
Conservation des rapports	115
Quarantaine pour les objets potentiellement infectés	116
Copie de sauvegarde des objets dangereux	116
Manipulation des objets en quarantaine	117
Conservation des objets de la quarantaine et de la sauvegarde	117
Kaspersky Security Network	117
Aspect extérieur du rapport	118
Éléments actifs de l'interface	118
Présentation graphique de Kaspersky Anti-Virus	119
Utilisation des profils de Kaspersky Anti-Virus	119
POSSIBILITES COMPLEMENTAIRES	121
Clavier virtuel	121
Disque de dépannage	122
Création d'un disque de dépannage	123
Démarrage de l'ordinateur à l'aide du disque de dépannage	123
Configuration du navigateur	124

Restauration après infection.....	125
Assistant de suppression des traces d'activité	126
RAPPORTS.....	127
Sélection du composant ou de la tâche pour la composition du rapport	127
Administration des groupes d'informations dans le rapport.....	128
Notification sur la disponibilité du rapport.....	129
Sélection du type d'événement	129
Présentation des données à l'écran.....	130
Présentation des données statistiques dans un tableau ou dans un graphique	131
Enregistrement du rapport dans un fichier	131
Utilisation du filtrage complexe.....	131
Recherche d'événements	132
NOTIFICATIONS	134
Un objet suspect a été détecté.....	135
La réparation de l'objet est impossible	136
Une procédure spéciale de réparation est requise	136
Un objet dangereux a été découvert dans le trafic.....	137
Un objet suspect a été détecté.....	137
Une activité dangereuse a été découverte dans le système	138
Un processus caché a été découvert.....	139
Une tentative d'accès à la base de registre système a été découverte.....	139
Une tentative de phishing a été découverte	140
Un lien suspect a été découvert	140
Découverte d'un certificat incorrect.....	140
VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE KASPERSKY ANTI-VIRUS.....	142
Virus d'essai EICAR et ses modifications.....	142
Test de la protection du trafic HTTP	143
Test de la protection du trafic SMTP.....	144
Vérification de l'exactitude de la configuration de l'Antivirus Fichiers.....	144
Vérification de l'exactitude de la configuration de la tâche d'analyse antivirus	145
UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE	146
Activation de l'application.....	147
Administration des composants de l'application et des tâches	148
Recherche de virus.....	150
Mise à jour de l'application.....	152
Annulation de la dernière mise à jour	153
Exportation des paramètres de protection	153
Importation des paramètres de protection.....	154
Lancement de l'application.....	154
Arrêt de l'application	154
Obtention du fichier de trace	154
Consultation de l'aide.....	155
Codes de retour de la ligne de commande.....	155
SUPPRESSION DES PROBLEMES.....	157
Création d'un rapport sur l'état du système.....	157
Création d'un fichier de trace.....	158
Envoi des fichiers de données.....	159

Exécution du script AVZ.....	159
REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK	161
UTILISATION D'UN CODE TIERS.....	165
CryptoEx S.A.R.L.	166
Bibliothèque fastscript 1.9	166
Bibliothèque pcre 7.4, 7.7	166
Bibliothèque GNU bison parser	167
Bibliothèque AGG 2.4	167
Bibliothèque OpenSSL 0.9.8d	167
Bibliothèque Gecko SDK 1.8	169
Bibliothèque zlib 1.2	169
Bibliothèque libpng 1.2.8, 1.2.29	169
Bibliothèque libnkfm 2.0.5	169
Bibliothèque expat 1.2, 2.0.1	169
Bibliothèque Info-ZIP 5.51	170
Bibliothèque Windows Installer XML (WiX) 2.0	170
Bibliothèque passthru	173
Bibliothèque filter	173
Bibliothèque netcfg	173
Bibliothèque pcre 3.0	173
Bibliothèque RFC1321-based (RSA-free) MD5 library	174
Bibliothèque Windows Template Library (WTL 7.5)	174
Bibliothèque libjpeg 6b	177
Bibliothèque libungif 3.0	178
Bibliothèque libxdr	178
Bibliothèque tiniconv - 1,0.0	179
Bibliothèque bzip2/libbzip2 1.0.5	183
Bibliothèque libspf2-1.2.9	184
Bibliothèque Protocol Buffer	184
GLOSSAIRE.....	186
CONTRAT DE LICENCE	194
KASPERSKY LAB	200
INDEX.....	201

INTRODUCTION

DANS CETTE SECTION

Distribution	9
Services pour les utilisateurs enregistrés	9
Configuration matérielle et logicielle requises	10

DISTRIBUTION

Vous pouvez acheter Kaspersky Anti-Virus chez nos revendeurs (version en boîte) ou en ligne (par exemple, <http://www.kaspersky.com/fr>, rubrique **Boutique en ligne**).

Si vous achetez le logiciel en boîte, vous recevrez :

- Une enveloppe cachetée contenant le cédérom d'installation avec les fichiers du logiciel et la documentation au format .pdf.
- La documentation en version "papier" présentée par les documents suivants : Manuel de l'utilisateur et Démarrage rapide.
- Contrat de licence (dépend de la région).
- La carte d'activation contenant le code d'activation et les instructions d'activation de l'application (dépend de la région).

Le contrat de licence est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les termes du contrat de licence, vous pouvez rendre la boîte avec le logiciel au magasin où vous l'avez acheté en échange du remboursement intégral. Dans ce cas, l'enveloppe contenant le cédérom ou les disquettes ne peut avoir été ouverte.

L'ouverture de l'enveloppe contenant le cédérom (ou les disquettes) d'installation marque votre accord avec les termes du contrat de licence.

Avant d'ouvrir l'enveloppe contenant le cédérom (ou les disquettes), veuillez lire attentivement le contrat de licence.

Si vous achetez Kaspersky Anti-Virus en ligne, vous copiez le logiciel depuis le site Internet de Kaspersky Lab. Cette distribution, outre le logiciel, reprend également ce guide. Le code d'activation vous sera envoyé par courrier électronique après le paiement.

SERVICES POUR LES UTILISATEURS ENREGISTRES

Kaspersky Lab offre à ses utilisateurs légitimes un vaste éventail de services qui leur permettent d'accroître l'efficacité de l'utilisation de l'application.

En obtenant une licence, vous devenez un utilisateur enregistré et vous pouvez bénéficier des services suivants pendant la durée de validité de la licence :

- Mise à jour toutes les heures des bases de l'application et accès aux nouvelles versions de ce logiciel ;
- Consultation par téléphone ou courrier électronique sur des questions liées à l'installation, à la configuration et à l'exploitation du logiciel ;
- Notifications de la sortie de nouveaux logiciels de Kaspersky Lab ou de l'émergence de nouveaux virus. Ce service est offert aux utilisateurs qui se sont abonnés au bulletin d'informations de Kaspersky Lab sur le site du service d'Assistance technique (<http://support.kaspersky.com/fr/subscribe>).

Aucune aide n'est octroyée pour les questions relatives au fonctionnement et à l'utilisation des systèmes d'exploitation, de logiciels tiers ou de diverses technologies.

CONFIGURATION MATERIELLE ET LOGICIELLE REQUISES

Pour que Kaspersky Anti-Virus 2010 puisse fonctionner normalement, l'ordinateur doit répondre aux exigences minimales suivantes :

Recommandations d'ordre général :

- 300 Mo d'espace disponible sur le disque dur.
- CD-ROM (pour l'installation de Kaspersky Anti-Virus 2010 depuis un cédérom).
- Microsoft Internet Explorer 6.0 ou suivant (pour la mise à jour des bases et des modules de l'application via Internet).
- Microsoft Windows Installer 2.0.
- ➡ *Microsoft Windows XP Home Edition (Service Pack 2), Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition :*
 - Processeur Intel Pentium 300 Mhz minimum (ou similaire).
 - 256 Mo de mémoire vive disponible.
- ➡ *Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate :*
 - Processeur Intel Pentium 800 Mhz 32 bits (x86)/ 64-bit (x64) minimum (ou similaire).
 - 512 Mo de mémoire vive disponible.

KASPERSKY ANTI-VIRUS 2010

Kaspersky Anti-Virus 2010 représente la nouvelle génération d'applications de protection des informations.

Ce qui distingue Kaspersky Anti-Virus 2010 des autres applications existantes, y compris des applications de Kaspersky Lab, c'est la démarche complexe adoptée pour la protection des informations stockées sur l'ordinateur de l'utilisateur.

DANS CETTE SECTION

Obtention d'informations sur l'application [11](#)

OBTENTION D'INFORMATIONS SUR L'APPLICATION

Si vous avez des questions sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Anti-Virus, vous pouvez trouver la réponse rapidement.

Kaspersky Lab offre diverses sources d'informations sur l'application. Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

Sources d'informations pour une aide autonome..... [11](#)

Contacter le service Ventes..... [12](#)

Contacter le service d'assistance technique..... [12](#)

SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

Vous pouvez consulter les sources d'informations suivantes sur l'application :

- La page de l'application sur le site de Kaspersky Lab ;
- La page de l'application sur le site du service d'assistance technique (dans la banque de solutions) ;
- La page du service d'assistance interactive ;
- L'aide électronique ;
- La documentation.

Page du site de Kaspersky Lab

http://www.kaspersky.com/fr/kaspersky_anti-virus

Cette page fournit des informations générales sur l'application, ses possibilités et ses particularités.

Page sur le site du service d'assistance technique (banque de solutions)

<http://support.kaspersky.com/fr/kav2010>

Cette page reprend des articles publiés par les experts du service d'assistance technique.

Ces articles proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application. Ils sont regroupés par sujets tels que "Utilisation des licences", "Configuration de la mise à jour des bases" ou "Suppression des échecs". Les articles peuvent répondre à des questions en rapport non seulement avec l'application mais également en rapport avec d'autres applications de Kaspersky Lab ; ils peuvent également fournir des nouvelles sur le service d'assistance technique dans son ensemble.

Service d'assistance interactive

La page de ce service propose une base fréquemment actualisée avec les questions fréquemment posées. L'utilisation de ce service requiert une connexion Internet.

Pour accéder à la page du service, dans la fenêtre principale de l'application, cliquez sur le lien **Assistance technique** et dans la fenêtre qui s'ouvre, cliquez sur le bouton **Assistance interactive**.

Aide électronique

La distribution de l'application reprend le fichier d'aide complète et contextuelle qui contient les informations sur la gestion de la protection de l'ordinateur : consultation de l'état de la protection, analyse de divers secteurs de l'ordinateur, exécution d'autres tâches ainsi que les informations relatives à chaque fenêtre de l'application : description des paramètres qui figurent dans chacune d'entre elles et liste des tâches exécutées.

Pour ouvrir le fichier d'aide, cliquez sur le bouton **Aide** dans la fenêtre qui vous intéresse ou sur la touche **<F1>** du clavier.

Documentation

La distribution de Kaspersky Anti-Virus reprend le document **Manuel de l'utilisateur** (au format .pdf). Ce document contient une description des fonctions et des possibilités de l'application ainsi que des principaux algorithmes de fonctionnement.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection, l'achat de Kaspersky Anti-Virus ou le renouvellement de la licence, vous pouvez contacter notre service Commercial en écrivant à :

info@fr.kaspersky.com ou consulter notre boutique en ligne sur :

<http://kaspersky.telechargement.fr/>

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Si vous avez acheté Kaspersky Anti-Virus, vous pouvez contacter les experts du service d'assistance technique par téléphone ou par Internet afin d'obtenir des informations sur cette application.

Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application et en cas d'infection, ils vous aideront à supprimer les dégâts provoqués par les applications malveillantes.

Avant de contacter le service d'assistance technique, veuillez prendre connaissance des règles d'assistance (<http://support.kaspersky.com/fr/support/rules>).

Assistance Technique en ligne

Vous pouvez retrouver toutes nos options de support à partir de notre portail de support :

<http://support.kaspersky.fr/kav2010>

Requête envoyée par voie électronique au service d'assistance technique

Les experts du service d'assistance technique vous transmettront leur réponse via votre Espace personnel (<https://my.kaspersky.com/fr>) et via le courrier électronique que vous aurez indiqué dans votre demande.

Décrivez le problème rencontré de la manière la plus détaillée possible dans le formulaire de contact. Saisissez les informations suivantes dans les champs obligatoires :

- **Type de demande.** Choisissez le sujet qui correspond le mieux à votre problème, par exemple « Suppression de virus » ou « Installation/désinstallation du programme ». Si aucune des propositions ne correspond à votre situation, choisissez l'option « Question générale »
- **Nom et version de l'application.**
- **Texte de la demande.** Décrivez le problème rencontré avec le plus de détails possibles.
- **Code client et mot de passe.** Saisissez le code client et le mot de passe que vous avez obtenu après l'enregistrement sur le site du service d'assistance technique.
- **Courrier électronique.** Il s'agit de l'adresse à laquelle les experts du service d'assistance technique enverront la réponse à votre demande.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM EN LIGNE

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse <http://forum.kaspersky.com>.

Une fois que vous avez accédé au forum, vous pouvez consulter les sujets publiés, écrire vos commentaires, créer de nouveaux sujets ou lancer des recherches.

NOUVEAUTES DE KASPERSKY ANTI-VIRUS 2010

Kaspersky Anti-Virus 2010 est un outil universel de protection des informations. Tous les canaux de transfert d'informations sont couverts par la protection sophistiquée. La souplesse de la configuration du moindre composant permet d'adapter Kaspersky Anti-Virus aux besoins particuliers de chaque utilisateur.

Voici une liste détaillée des nouveautés introduites dans Kaspersky Anti-Virus 2010.

Nouveautés au niveau de la protection :

- Le nouveau composant Antivirus IM ("Chat") (cf. page [66](#)) garantit une utilisation sans danger de plusieurs systèmes de messagerie instantanée. Le composant analyse les messages sur la présence des objets malveillants.
- Kaspersky Anti-Virus propose un module d'analyse des liens (cf. page [63](#)) qui est administré par l'Antivirus Internet. Le module analyse tous les liens sur une page afin de voir s'il s'agit de liens suspects ou de phishing. Le module est intégré aux navigateurs Microsoft Internet Explorer et Mozilla Firefox sous la forme d'un plug-in.
- Le contrôle de l'accès aux sites de phishing et la protection contre les attaques de phishing s'opèrent via l'analyse des liens contenus dans les messages et sur les pages Web, ainsi que lors des tentatives d'ouverture de sites, par rapport à la base des URL de phishing. La recherche des URL dans les bases de phishing est une fonction offerte par l'Antivirus Internet (cf. page [62](#)) et l'Antivirus IM ("Chat") (cf. page [67](#)).
- La liste des analyses contient un nouvel instrument, à savoir la Recherche de Vulnérabilités (cf. page [82](#)) qui facilite la recherche et la suppression des menaces pour la sécurité et des vulnérabilités dans les applications installées et les paramètres du système d'exploitation.

Nouveautés de l'interface :

- Nouvelle conception de l'administration de la protection avec l'introduction du centre de protection (Protection). La protection de l'ordinateur est assurée à trois niveaux : au niveau des fichiers et des données personnelles, au niveau des objets du système d'exploitation et des applications installées et au niveau de l'utilisation du réseau. Un groupe de composants distincts est responsable pour chaque aspect de la protection. La centrale de protection permet d'évaluer la participation de chaque composant dans la protection d'une ressource particulière et d'accéder rapidement à la configuration de ses paramètres.
- Les Assistants et les outils (cf. page [18](#)) qui aident à résoudre les tâches spécifiques pour la sécurité de l'ordinateur sont repris dans une section particulière **Utilitaires+**.

CONCEPT DE LA PROTECTION DE VOTRE ORDINATEUR

Kaspersky Anti-Virus protège votre ordinateur contre les virus connus ou nouveaux. Chaque type de menace est traité par un composant distinct de l'application. Une telle conception de la protection permet de réaliser une configuration souple de l'application en fonction des besoins concrets de chaque utilisateur ou entreprise.

Kaspersky Anti-Virus propose les outils suivants pour la protection :

- Les composants de la protection (cf. page [15](#)) qui assurent la protection :
 - Des fichiers et des données personnelles ;
 - Du système ;
 - De l'utilisation du réseau.
- Les tâches d'analyse (cf. page [17](#)) qui permettent de rechercher la présence éventuelle de virus dans des fichiers, des répertoires, des disques ou des secteurs déterminés ou de lancer une analyse complète de l'ordinateur.
- La mise à jour (cf. page [17](#)) qui garantit l'actualité des modules internes de l'application et des bases utilisées pour identifier les applications malveillantes, repérer les attaques de réseau et isoler les messages non sollicités.
- Les assistants et les outils (cf. page [18](#)) qui facilitent l'exécution des tâches découlant du fonctionnement de Kaspersky Anti-Virus.
- Les fonctions de service (cf. page [18](#)) qui offrent des informations sur l'utilisation des applications et qui permettent d'élargir leurs fonctions.

DANS CETTE SECTION

Composants de la protection.....	15
Tâches de recherche d'éventuels virus	17
Mise à jour.....	17
Protection des données et de l'activité en ligne	18
Assistants et outils	18
Fonctions de service de l'application.....	18

COMPOSANTS DE LA PROTECTION

La protection de votre ordinateur en temps réel est garantie par les composants de la protection :

Antivirus Fichiers (cf. page [42](#))

L'Antivirus Fichiers contrôle le système de fichiers de l'ordinateur. Il analyse tous les fichiers ouverts, exécutés ou enregistrés sur l'ordinateur et sur tous les disques connectés. Chaque requête adressée à un fichier est interceptée par Kaspersky Anti-Virus et le fichier est soumis à une recherche des virus connus. Il sera possible de continuer à

utiliser le fichier uniquement si celui-ci est sain ou s'il a pu être réparé par l'application. Si la réparation du fichier est impossible pour une raison quelconque, le fichier sera supprimé mais une copie sera enregistrée dans la sauvegarde ou placée en quarantaine.

Antivirus Courrier (cf. page [52](#))

L'Antivirus Courrier analyse tout le courrier entrant et sortant de votre ordinateur. Il recherche la présence éventuelle d'applications malveillantes dans les messages électroniques. Le message sera délivré au destinataire uniquement s'il ne contient aucun objet dangereux. Le composant recherche également la présence éventuelle d'attaques d'hameçonnage dans les messages électroniques.

Antivirus Internet (cf. page [59](#))

L'Antivirus Internet intercepte et bloque l'exécution des scripts dans les pages Web si ceux-ci constituent une menace. Tout le trafic HTTP est également soumis à un contrôle strict. Le composant recherche également la présence éventuelle d'attaques d'hameçonnage dans les pages Web.

Antivirus IM ("Chat") (cf. page [66](#))

L'Antivirus IM garantit la sécurité de l'utilisation des messages instantanées. Le composant protège les informations envoyées vers votre ordinateur via les protocoles des clients de messagerie instantanée. Antivirus IM vous protège pendant l'utilisation de nombreux clients de messagerie instantanée.

Défense Proactive (cf. page [69](#))

La défense proactive permet d'identifier une nouvelle application malveillante avant qu'elle n'ait eu le temps de provoquer des dégâts. Le composant repose sur la surveillance et l'analyse du comportement de toutes les applications installées sur l'ordinateur. En fonction des actions exécutées, Kaspersky Antivirus décide si l'application constitue un danger potentiel ou non. Ainsi, l'ordinateur est protégé non seulement contre les virus connus mais également contre les nouveaux virus qui n'ont pas encore été étudiés.

Anti-phishing

Composant intégré à l'Antivirus Internet et l'Antivirus IM qui permet de vérifier si une URL appartient à la liste des URL suspectes ou de phishing.

Certains composants de la protection sont disponibles uniquement dans Kaspersky Internet Security 2010. Parmi eux :

Contrôle des Applications

Le Contrôle des Applications enregistre les actions réalisées par les applications dans le système et régleme l'activité des applications sur la base du groupe dans lequel le composant place cette application. Un ensemble de règles a été défini pour chaque groupe d'applications. Ces règles définissent l'accès des applications à diverses ressources.

Pare-Feu

Le Pare-feu vous protège pendant l'utilisation des réseaux locaux et d'Internet. Le composant filtre toute l'activité de réseau selon deux types de règles : *les règles pour les applications et les règles pour les paquets*.

Défense Proactive

La défense proactive permet d'identifier une nouvelle application malveillante avant qu'elle n'ait eu le temps de provoquer des dégâts. Le composant repose sur la surveillance et l'analyse du comportement de toutes les applications installées sur l'ordinateur. En fonction des actions exécutées, Kaspersky Anti-Virus décide si l'application constitue un danger potentiel ou non. Ainsi, l'ordinateur est protégé non seulement contre les virus connus mais également contre les nouveaux virus qui n'ont pas encore été étudiés.

Protection contre les attaques de réseau

La Prévention des intrusions est lancée au démarrage du système d'exploitation et surveille l'activité du trafic entrant caractéristique des attaques de réseau. Dès qu'il détecte une tentative d'attaque contre votre ordinateur, Kaspersky Anti-Virus bloque toute activité de réseau de l'ordinateur qui vous attaque.

Anti-Spam

L'Anti-Spam s'intègre au client de messagerie de votre ordinateur et recherche la présence éventuelle de messages non sollicités dans tout le courrier entrant. Tous les messages non sollicités identifiés sont marqués par un objet particulier. Il est possible également de configurer l'Anti-Spam pour le traitement du courrier indésirable (suppression automatique, enregistrement dans un répertoire spécial, etc.). Le composant recherche également la présence éventuelle d'attaques d'hameçonnage dans les messages électroniques.

Surveillance du réseau

Ce composant a été développé pour consulter en temps réel les informations relatives à l'activité de réseau.

Anti-bannière

Anti-bannière bloque les messages publicitaires situés sur des bannières spéciales dans l'interface de divers programmes installés sur votre ordinateur ou sur Internet.

Contrôle Parental

Le Contrôle Parental est un composant de l'application qui permet de contrôler l'accès des utilisateurs aux ressources Internet. La fonction principale du Contrôle Parental est de limiter l'accès aux sites pour adultes, aux sites pornographiques, faisant l'apologie des armes et des drogues, incitant à la cruauté, à la violence, etc. ainsi qu'aux sites pouvant entraîner une perte de temps (chats, jeux) ou d'argent (magasins en ligne, sites de ventes aux enchères).

TACHES DE RECHERCHE D'EVENTUELS VIRUS

Outre la protection de toutes les sources d'introduction d'applications malveillantes, il est primordial de réaliser à intervalle régulier une analyse de votre ordinateur. Cette opération s'impose pour exclure la possibilité de propager des applications malveillantes qui n'auraient pas été décelées par les composants de la protection en raison, par exemple, d'un niveau de protection faible ou pour toute autre raison.

Kaspersky Anti-Virus contient les tâches suivantes pour la recherche de virus :

- **Analyse des objets.** Analyse des objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet du système de fichiers de l'ordinateur.
- **Analyse Complète.** Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.
- **Analyse Rapide.** Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation.

MISE A JOUR

Afin d'être toujours prêt à faire face à n'importe quelle activité de réseau, à supprimer des virus ou d'autres applications dangereuses, il faut maintenir Kaspersky Anti-Virus à jour. Le composant **Mise à jour** a été développé à cette fin. Il est chargé de la mise à jour des bases et des modules de l'application utilisés.

Le service de copie des mises à jour permet d'enregistrer les mises à jour des bases et des modules de l'application récupérées sur les serveurs de Kaspersky Lab dans un répertoire local et puis, d'octroyer l'accès à ce répertoire aux autres ordinateurs du réseau dans le but d'économiser le trafic Internet.

PROTECTION DES DONNEES ET DE L'ACTIVITE EN LIGNE

Kaspersky Anti-Virus protège les données de votre ordinateur contre les applications malveillantes et l'accès non autorisé et garantit également la sécurité de l'accès au réseau local et à Internet.

Les objets protégés sont scindés en trois groupes :

- Les fichiers, les données personnelles, les paramètres d'accès à diverses ressources (nom d'utilisateur et mot de passe), les informations relatives aux cartes bancaires, etc. La protection de ces objets est garantie par l'Antivirus Fichiers et la Défense proactive.
- Les applications installées sur l'ordinateur et les objets du système d'exploitation. L'Antivirus Courrier, l'Antivirus Internet, l'Antivirus IM ("Chat") et la Défense proactive assurent la protection de ces objets.
- Utilisation du réseau : consultation de sites, utilisation de systèmes de paiement en ligne, protection du courrier contre les messages non sollicités et les virus, etc. L'Antivirus Courrier, l'Antivirus Internet, l'Antivirus IM ("Chat") et l'Anti-phishing assurent la protection de ces objets.

ASSISTANTS ET OUTILS

Garantir la protection de l'ordinateur est une tâche complexe qui requiert des connaissances sur les particularités de fonctionnement du système d'exploitation et sur les moyens d'exploiter ses points faibles. De plus, le volume important des informations sur la protection du système et la diversité de celles-ci complique l'analyse et le traitement.

Pour faciliter l'exécution de tâches spécifiques pour la sécurité de l'ordinateur, Kaspersky Anti-Virus contient plusieurs assistants et outils :

- Assistant de configuration du navigateur (cf. page [124](#)) qui analyse les paramètres du navigateur Microsoft Internet Explorer et qui les évalue avant tout du point de vue de la sécurité.
- Assistant de restauration après infection (cf. page [125](#)) permet de liquider les traces de la présence d'objets malveillants dans le système.
- Assistant de suppression des traces d'activité (cf. page [126](#)) recherche et supprime les traces d'activité de l'utilisateur dans le système ainsi que les paramètres du système d'exploitation qui permettent d'accumuler des données sur l'activité de l'utilisateur.
- Disque de dépannage (cf. page [122](#)) est prévu pour le contrôle et la réparation des ordinateurs (compatibles x86) infectés. Il intervient dans les cas d'infection qui rendent la réparation de l'ordinateur impossible à l'aide des logiciels antivirus ou des outils de réparation.
- Recherche de Vulnérabilités (cf. page [82](#)) pose un diagnostic sur la sécurité de l'ordinateur et recherche les vulnérabilités dans le système d'exploitation et les applications installées.
- Clavier virtuel (cf. page [121](#)) qui permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.

FONCTIONS DE SERVICE DE L'APPLICATION

Kaspersky Anti-Virus intègre diverses fonctions de service. Ces fonctions visent à maintenir l'application à jour, à élargir les possibilités d'utilisation et à faciliter l'utilisation.

Fichiers de données et rapports

Un rapport est créé sur chaque composant de la protection, chaque analyse ou chaque mise à jour pendant l'utilisation de l'application. Ce rapport contient des informations sur les opérations exécutées et sur les résultats des tâches, ce qui vous permet de toujours connaître en détails le fonctionnement de n'importe quel composant de Kaspersky Anti-Virus. En cas de problèmes, les rapports peuvent être envoyés à Kaspersky Lab où les experts pourront étudier la situation plus en détails et vous aider à résoudre le problème le plus vite possible.

Tous les objets suspects du point de vue de la sécurité sont placés par Kaspersky Anti-Virus dans un répertoire spécial : la *quarantaine*. Les objets sont conservés sous forme chiffrée afin d'éviter l'infection de l'ordinateur. Vous pouvez soumettre ces objets à une analyse, les restaurer dans leur emplacement d'origine, les supprimer ou les ajouter vous-même à la quarantaine. Tous les objets considérés comme sains suite à l'analyse sont restaurés automatiquement dans leur emplacement d'origine.

La *sauvegarde* abrite les copies des objets réparés ou supprimés par Kaspersky Anti-Virus. Ces copies sont créées au cas où il faudrait restaurer les objets ou reproduire le scénario de l'infection. Les copies de sauvegarde des objets sont conservées également sous forme chiffrée afin d'éviter l'infection de l'ordinateur.

Vous pouvez restaurer l'objet depuis la sauvegarde vers son emplacement d'origine ou supprimer la copie.

Licence

Au moment d'acheter Kaspersky Antivirus, vous et Kaspersky Lab signez un contrat de licence qui vous donne le droit d'utiliser l'application, de recevoir les mises à jour des bases de l'application et de contacter le service d'assistance technique durant une période déterminée. La durée d'utilisation ainsi que toute autre information requise pour le fonctionnement de l'application figurent dans la licence.

Le menu **Licence** vous permet d'obtenir des informations détaillées sur la licence que vous utilisez, d'acheter une nouvelle licence ou de renouveler la licence en cours.

Assistance technique

Tous les utilisateurs enregistrés de Kaspersky Anti-Virus peuvent utiliser le service d'assistance technique. Pour connaître les conditions d'octroi de l'assistance, utilisez le menu **Assistance technique**.

Grâce aux liens correspondant, vous pouvez accéder au forum des utilisateurs des applications de Kaspersky Lab ou envoyer au service d'assistance technique un message sur une erreur ou un commentaire sur le fonctionnement de l'application en remplissant un formulaire spécial sur le site.

Vous avez également accès au service d'assistance technique en ligne, à l'Espace personnel de l'utilisateur et, bien évidemment, aux consultations téléphoniques avec nos collaborateurs qui sont toujours prêts à vous aider dans votre utilisation de Kaspersky Anti-Virus.

INSTALLATION DE KASPERSKY ANTI-VIRUS SUR L'ORDINATEUR

L'installation de l'application se déroule en mode interactif à l'aide de l'Assistant d'installation de l'application.

Avant de lancer l'installation, il est conseillé de quitter toutes les applications en cours d'exécution.

Pour installer l'application, lancez le fichier de distribution (extension *.exe) sur le cédérom du logiciel.

L'installation de Kaspersky Anti-Virus au départ d'une distribution téléchargée depuis Internet est identique à l'installation depuis le cédérom.

Vient ensuite la recherche du paquet d'installation de Kaspersky Anti-Virus (fichier doté de l'extension *.msi). Si le fichier est présent, le système vérifiera l'existence d'une version plus récente sur les serveurs de Kaspersky Lab via Internet. Si le fichier du paquet d'installation est introuvable, vous serez invité à le télécharger. L'installation de Kaspersky Anti-Virus sera lancée à la fin du téléchargement. En cas de refus du téléchargement, l'installation de l'application se poursuivra en mode normal.

Le programme d'installation se présente sous la forme d'un Assistant. Chaque fenêtre contient une sélection de boutons qui permettent d'administrer le processus d'installation. Voici une brève description de leur fonction :

- **Suivant** : exécute l'action et passe à l'étape suivante de l'installation.
- **Précédent** : revient à l'étape précédente de l'installation.
- **Annuler** : annule l'installation du logiciel.
- **Terminer** : termine la procédure d'installation de l'application.

Examinons en détail chacune des étapes de la procédure d'installation.

DANS CETTE SECTION

Etape 1. Recherche d'une version plus récente de l'application	21
Etape 2. Vérification des configurations minimum requises pour l'installation	21
Etape 3. Sélection du type d'installation	22
Etape 4. Lecture du Contrat de licence	22
Etape 5. Règlement d'utilisation de Kaspersky Security Network	22
Etape 6. Sélection du répertoire d'installation	22
Etape 7. Sélection des composants de l'application à installer	23
Etape 8. Utilisation des paramètres de l'application conservés de l'installation antérieure	23
Etape 9. Recherche d'autres logiciels antivirus	24
Etape 10. Derniers préparatifs pour l'installation de l'application	24
Etape 11. Fin de la procédure d'installation	24

ÉTAPE 1. RECHERCHE D'UNE VERSION PLUS RÉCENTE DE L'APPLICATION

Avant l'installation une recherche d'une version plus actuelle de Kaspersky Anti-Virus sur les serveurs des mises à jour de Kaspersky Lab s'effectue.

Si les serveurs de Kaspersky Lab n'hébergent pas une version plus récente, l'Assistant d'installation de la version actuelle est lancé.

Si les serveurs de mises à jour hébergent une version plus récente, vous serez invité à la télécharger et à l'installer sur votre ordinateur. Si vous refusez d'installer la version plus récente, l'Assistant d'installation de la version actuelle sera lancé. Si vous décidez d'installer la nouvelle version, les fichiers de la distribution seront copiés sur l'ordinateur et l'Assistant d'installation sera lancé automatiquement.

ÉTAPE 2. VÉRIFICATION DES CONFIGURATIONS MINIMUM REQUISES POUR L'INSTALLATION

Avant de procéder à l'installation de l'application, le système vérifie si le système d'exploitation et les Service Pack installés répondent aux exigences pour l'installation. Également, la présence du logiciel requis ainsi que des droits d'installation du logiciel est vérifiée.

Si une des conditions n'est pas remplie, le message de circonstance apparaîtra. En ce cas, avant l'installation de l'application de Kaspersky Lab, il est recommandé d'installer les paquets des mises à jour requis à l'aide du service Windows Update et les programmes nécessaires.

ETAPE 3. SELECTION DU TYPE D'INSTALLATION

Si votre système répond parfaitement aux exigences, s'il n'existe pas une version plus récente de l'application sur les serveurs de mise à jour de Kaspersky Lab ou si vous avez décidé de ne pas installer cette version plus récente, l'Assistant d'installation de la version actuelle s'ouvre.

Cette étape d'installation correspond à la sélection du type d'installation qui vous convient le mieux :

- *Installation rapide.* Si vous choisissez cette option (la case ☒ **Installation personnalisée** est cochée), l'application sera installée en entier sur l'ordinateur avec les paramètres de protection recommandés par les experts de Kaspersky Lab. L'Assistant de configuration (à la page [26](#)) sera lancé à la fin de l'installation.
- *Installation personnalisée.* Dans ce cas de figure (la case ☒ **Installation personnalisée** est cochée), vous êtes invité à sélectionner les composants de l'application que vous souhaitez installer, et à désigner le répertoire dans lequel l'application sera installée, ainsi qu'à activer l'application et à la configurer à l'aide d'un Assistant spécial.

Quand vous sélectionnez la première option, l'Assistant d'installation de l'application vous proposera de prendre connaissance avec le contrat de licence ainsi qu'avec le règlement d'utilisation de Kaspersky Security Network. Ensuite, le programme sera installé sur votre ordinateur.

Dans le deuxième cas, vous devrez saisir ou confirmer certaines données à chaque étape de l'installation.

Pour poursuivre l'installation, cliquez sur **Suivant**. Pour annuler l'installation, cliquez sur le bouton **Annuler**.

ETAPE 4. LECTURE DU CONTRAT DE LICENCE

Cette étape vous recommande de prendre connaissance avec le contrat de licence qui est conclu entre vous et Kaspersky Lab.

Lisez-le attentivement et si vous n'avez aucune objection à formuler, cliquez sur le bouton **J'accepte**. L'installation de l'application sur votre ordinateur se poursuivra.

Pour arrêter l'installation, cliquez sur le bouton **Annuler**.

ETAPE 5. REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Cette étape vous offre la possibilité de participer au programme Kaspersky Security Network. La participation dans le programme prévoit l'envoi de l'information sur les nouvelles menaces, découvertes sur votre ordinateur, envoi de l'identificateur unique, attribué à votre ordinateur par Kaspersky Anti-Virus, et de l'information sur le système à Kaspersky Lab. Vous recevrez la garantie que des données personnelles ne seront pas transmises.

Lisez attentivement le règlement d'utilisation de Kaspersky Security Network. Si vous n'avez aucune objection à formuler, cochez la case ☒ **J'accepte les conditions de participation à Kaspersky Security Network**.

Cliquez sur **Suivant**. L'installation se poursuit.

ETAPE 6. SELECTION DU REPERTOIRE D'INSTALLATION

Cette étape de l'Assistant apparaît uniquement si vous avez sélectionné l'installation personnalisée (cf. section "Etape 3. Sélection du type d'installation" à la page [22](#)).

Vous devez désigner le répertoire dans lequel l'application sera installée. Le chemin proposé par défaut est le suivant :

- <Disque> \ Program Files \ Kaspersky Lab \ Kaspersky Anti-Virus 2010 : pour les systèmes 32 bits.
- <Disque> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus 2010 : pour les systèmes 64 bits.

Vous pouvez choisir un autre dossier à l'aide du bouton **Parcourir** qui ouvre la fenêtre standard de sélection de dossier ou saisir le chemin d'accès dans le champ prévu à cet effet.

N'oubliez pas que si vous saisissez manuellement le chemin d'accès complet au dossier d'installation, le nom ne pourra pas compter plus de 200 caractères ni contenir des caractères spéciaux.

Pour poursuivre l'installation, cliquez sur **Suivant**.

ÉTAPE 7. SÉLECTION DES COMPOSANTS DE L'APPLICATION A INSTALLER

Cette étape de l'Assistant apparaît uniquement si vous avez sélectionné l'installation personnalisée (cf. section "Étape 3. Sélection du type d'installation" à la page [22](#)).

En cas d'installation personnalisée, vous devez désigner les composants de l'application que vous souhaitez installer. Tous les composants de Kaspersky Anti-Virus sont sélectionnés par défaut pour l'installation : les composants de protection, les tâches d'analyse et les mises à jour.

Les brèves informations fournies pour chaque composant vous aideront à choisir les composants que vous ne souhaitez pas installer. Il suffit de sélectionner le composant dans la liste et de lire les informations qui apparaissent dans le champ inférieur. Il s'agit d'une brève description de la fonction du composant et de l'espace requis sur le disque.

Si vous décidez de ne pas installer un composant quelconque, ouvrez le menu contextuel en cliquant sur l'icône située à côté du nom du composant puis sélectionnez le point **Le composant sera inaccessible**. N'oubliez pas qu'en annulant l'installation d'un composant quelconque, vous vous privez de la protection contre toute une série de programmes dangereux.

Afin de sélectionner le composant à installer, ouvrez le menu contextuel en cliquant sur l'icône située à côté du nom du composant et sélectionnez le point **Le composant sera installé sur un disque dur local**.

Une fois que la sélection des composants est terminée, cliquez sur le bouton **Suivant**. Pour revenir à la liste des composants à installer par défaut, cliquez sur le bouton **Abandon**.

ÉTAPE 8. UTILISATION DES PARAMÈTRES DE L'APPLICATION CONSERVES DE L'INSTALLATION ANTERIEURE

Cette étape vous permet de décider si vous souhaitez utiliser les paramètres de protection, si elles ont été préservées sur votre ordinateur, lors de la suppression de la version antérieure de Kaspersky Anti-Virus.

Examinons en détail la manière d'utiliser les possibilités décrites ci-dessus.

Si une version antérieure de Kaspersky Anti-Virus était installée sur l'ordinateur et que lors de sa suppression, vous avez conservé les bases de l'application, vous pouvez les activer en vue d'une utilisation avec la nouvelle version installée. Pour ce faire, cochez la case ☒ **Bases de l'application**. Les bases reprises dans la distribution de l'application ne seront pas copiées sur l'ordinateur.

Pour utiliser les paramètres de protection configurés dans la version antérieure et préservés sur l'ordinateur, cochez la case ☒ **Paramètres de fonctionnement de l'application.**

ETAPE 9. RECHERCHE D'AUTRES LOGICIELS ANTIVIRUS

Cette étape correspond à la recherche d'autres logiciels antivirus installés, y compris d'autres logiciels de Kaspersky Lab, dont l'utilisation simultanée avec cette application pourrait entraîner des conflits.

Si de tels programmes existent sur l'ordinateur, une liste reprenant leur nom s'affichera. Vous serez invité à les supprimer avant de poursuivre l'installation.

Sous la liste des logiciels antivirus découverts, vous pouvez choisir une des options de suppression : automatiquement ou manuellement.

Si une application de Kaspersky Lab version 2009 figure dans la liste, il est conseillé de conserver le fichier de licence utilisé par cette application avant de la supprimer manuellement. Vous pourrez l'appliquer à la nouvelle version de l'application. Il est également conseillé de conserver les objets de la quarantaine et de la sauvegarde. Ils seront placés automatiquement dans la quarantaine de la nouvelle version de Kaspersky Anti-Virus et vous pourrez continuer à les manipuler.

En cas de suppression automatique d'une application de la version 2009, les informations relatives à l'activation seront conservées par le programme et réutilisées lors de l'installation de la version 2010.

Pour poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 10. DERNIERS PREPARATIFS POUR L'INSTALLATION DE L'APPLICATION

Lors de cette étape, vous êtes invité à réaliser les derniers préparatifs pour l'installation de l'application.

En cas d'installation initiale et personnalisée (cf. section "Etape 3. Sélection du type d'installation" à la page [22](#)) de l'application, il est déconseillé de désélectionner la case ☒ **Protéger l'installation de l'application**. Si, lors de l'installation les erreurs surviennent, la protection activée permet de remettre correctement l'installation à l'état antérieur. En cas de nouvelle tentative d'installation, il est conseillé de désélectionner cette case.

En cas d'installation à distance via *Windows Bureau distant*, il est conseillé de désélectionner la case ☒ **Protéger l'installation de l'application**. Si cette case est cochée, l'installation peut ne pas être réalisée ou être réalisée de manière incorrecte.

Pour poursuivre l'installation, cliquez sur **Installer**.

Durant l'installation des composants de Kaspersky Anti-Virus qui interceptent le trafic de réseau, les connexions de réseau ouvertes sont interrompues. La majorité des connexions interrompues seront rétablies après un certain temps.

ETAPE 11. FIN DE LA PROCEDURE D'INSTALLATION

La fenêtre **Fin de l'installation** contient des informations sur la fin du processus d'installation de l'application.

Pas suivant – c'est la configuration de l'application pour assurer la protection maximale de votre information sur l'ordinateur. L'Assistant de configuration (cf. section "Assistant de configuration de l'application" à la page [26](#)) aidera à configurer Kaspersky Anti-Virus rapidement et correctement.

Cliquez sur le bouton **Suivant** pour passer à la configuration de l'application.

PREMIERE UTILISATION

Une des principales tâches des experts de Kaspersky Lab dans le cadre du développement de Kaspersky Anti-Virus fut de veiller à la configuration optimale de tous les paramètres du logiciel. Ainsi, tout utilisateur, quelles que soient ses connaissances en informatique, peut assurer la protection de son ordinateur dès l'installation du logiciel sans devoir s'encombrer de la configuration.

Afin de rendre l'utilisation plus conviviale, nous avons tenté de regrouper les étapes de configuration préliminaire au sein d'une interface unique : l'Assistant de configuration de l'application (cf. section "Assistant de configuration de l'application" à la page [26](#)) qui démarre à la fin de la procédure d'installation de l'application. Grâce aux instructions de l'Assistant, vous pourrez activer Kaspersky Anti-Virus, configurer les paramètres de la mise à jour, limiter l'accès au programme à l'aide d'un mot de passe et configurer d'autres paramètres.

Votre ordinateur peut être infecté par des programmes malveillants avant l'installation de l'application. Afin de découvrir les programmes malveillants présents, lancez l'analyse de l'ordinateur.

Les valeurs des paramètres de votre ordinateur peuvent être corrompues suite à l'action de programmes malveillants ou aux échecs du système. Lancez la tâche de recherche de vulnérabilités (cf. section "Recherche de vulnérabilités sur l'ordinateur" à la page [30](#)) afin de trouver des vulnérabilités dans les logiciels installés ou des anomalies dans les configurations du système.

Les bases livrées avec l'application peuvent être dépassées au moment de l'installation de celle-ci. Lancez la mise à jour de l'application (au cas où cela n'aurait pas été réalisé à l'aide de l'Assistant de configuration ou automatiquement après l'installation de l'application).

Le composant Anti-Spam, qui fait partie de l'application, identifie les messages non sollicités à l'aide d'un algorithme d'auto-apprentissage. Lancez l'Assistant d'apprentissage d'Anti-Spam afin de configurer le composant pour votre correspondance.

Une fois que les opérations décrites ci-dessus auront été réalisées, Kaspersky Anti-Virus sera prêt à fonctionner. Pour évaluer le niveau de protection de votre ordinateur, utilisez l'Assistant d'administration de la sécurité.

DANS CETTE SECTION

Assistant de configuration de l'application	26
Mise à jour de l'application	29
Recherche de virus sur l'ordinateur	30
Recherche de vulnérabilités sur l'ordinateur	30
Administration de la licence	30
Abonnement pour le renouvellement automatique de la licence	31
Participation au Kaspersky Security Network	32
Administration de la sécurité	33
Etat de la protection	35
Suspension de la protection	35

ASSISTANT DE CONFIGURATION DE L'APPLICATION

L'Assistant de configuration de l'application démarre pendant l'installation. Son rôle est de vous aider à réaliser la configuration initiale de Kaspersky Anti-Virus sur la base des particularités et des tâches de votre ordinateur.

L'interface de l'Assistant de configuration se présente sous la forme d'une succession de fenêtres (étapes) et la navigation entre celles-ci s'opère à l'aide des liens **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le lien **Annuler**.

VOICI, EN DETAILS, LES ETAPES DE L'ASSISTANT :

Etape 1. Activation de l'application.....	26
Etape 2. Sélection du mode de protection.....	28
Etape 3. Configuration de la mise à jour de l'application.....	28
Etape 4. Restriction de l'accès à l'application.....	29
Etape 5. Sélection des menaces identifiées.....	29
Etape 6. Fin de l'Assistant.....	29

ETAPE 1. ACTIVATION DE L'APPLICATION

La procédure d'activation de l'application consiste en l'enregistrement de la licence à l'aide de l'installation du fichier clé. Sur la base de la licence l'application déterminera l'existence des droits d'utilisation et de leur durée.

La licence contient les informations de service indispensables pour assurer le parfait fonctionnement de Kaspersky Anti-Virus, ainsi que des renseignements complémentaires :

- les informations sur l'assistance technique (qui l'assure et comment l'obtenir) ;
- le nom et le numéro du fichier clé ainsi que sa date d'expiration.

Une connexion à Internet est indispensable pour activer l'application.

Afin de recevoir le fichier de licence pendant l'activation, il faut posséder le code d'activation. Le code d'activation est fourni à l'achat de l'application. Vous pouvez activer Kaspersky Anti-Virus d'une des manières suivantes :

- **Activer la version commerciale.** Sélectionnez cette option si vous avez acheté une version commerciale du logiciel et que vous avez reçu le code d'activation. Vous recevrez, sur la base de ce code, le fichier de licence qui vous donnera accès à l'ensemble des fonctions de l'application pendant toute la durée de validité de la licence.
- **Activer la version d'évaluation.** Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter la version commerciale. Vous recevrez un fichier de licence gratuite dont la durée de validité sera limitée par la licence associée à la version d'évaluation de l'application.
- **Activer plus tard.** Si vous choisissez cette option, l'activation de Kaspersky Anti-Virus sera ignorée. Le programme sera installé sur l'ordinateur et vous aurez accès à toutes les fonctions, à l'exception de la mise à jour (vous pourrez actualiser Kaspersky Anti-Virus une seule fois après l'installation). L'option **Activer plus tard** est accessible uniquement au premier lancement de l'Assistant d'activation, juste après l'installation de l'application.

Si Kaspersky Anti-Virus avait été installé puis supprimé sans perdre les données relatives à l'activation, alors cette étape n'est pas présentée. Dans ce cas, l'Assistant de configuration récupère automatiquement les informations relatives à la licence et les affiche dans la fenêtre de l'Assistant (cf. page [27](#)).

VOIR EGALEMENT

Activation de la version commerciale	27
Activation de la version d'évaluation	27
Fin de l'activation	27

ACTIVATION DE LA VERSION COMMERCIALE

Si vous choisissez cette option, l'activation du programme s'opère via le serveur Web de Kaspersky Lab. Une connexion à Internet est nécessaire dans ce cas.

L'activation repose sur la saisie du code d'activation que vous recevez par courrier électronique après avoir acheté Kaspersky Anti-Virus dans un magasin en ligne. Si vous avez acheté le logiciel dans un magasin traditionnel, le code d'activation est repris sur la carte d'activation.

Le code d'activation se présente sous la forme d'une série de chiffres et de lettres séparés par des traits d'union en 4 groupes de cinq chiffres, sans espace : par exemple, 11111-11111-11111-11111. N'oubliez pas que le code doit être saisi en caractères romains.

L'Assistant d'activation établit une connexion avec le serveur d'activation de Kaspersky Lab sur Internet et les envoie votre code d'activation, ensuite le code est analysé. Si le code d'activation est valide, l'assistant télécharge le fichier de licence qui s'installe alors automatiquement. L'activation est terminée et une fenêtre s'affiche avec les informations détaillées sur la licence acquise.

En cas d'activation de l'abonnement, outre les informations citées ci-dessus, les données relatives à l'état de l'abonnement (cf. section "Abonnement pour le renouvellement automatique de la licence" à la page [31](#)) seront également disponibles.

Si le code d'activation n'est pas reconnu, un message vous le signalera. Dans ce cas, contactez la société où vous avez acheté Kaspersky Anti-Virus pour obtenir des informations.

Si le nombre d'activations autorisé pour le code a été dépassé, un message s'affiche à l'écran. Le processus d'activation est alors interrompu et l'application vous redirige vers l'assistance technique de Kaspersky Lab.

Si une erreur s'est produite au moment de se connecter au serveur d'activation ou si vous n'avez pas pu récupérer le fichier de licence, contactez le service d'assistance technique.

ACTIVATION DE LA VERSION D'EVALUATION

Sélectionnez cette option si vous souhaitez installer une version d'évaluation de Kaspersky Anti-Virus avant de décider d'acheter la version commerciale. Vous recevrez un fichier de licence gratuit dont la durée de validité sera déterminée par le contrat de licence de la version d'évaluation de l'application. A l'expiration du délai de validité de la licence d'évaluation, la possibilité d'activation secondaire de la version d'évaluation sera inaccessible.

Si une erreur s'est produite au moment de se connecter au serveur d'activation ou si vous n'avez pas pu récupérer le fichier de licence, contactez le service d'assistance technique.

FIN DE L'ACTIVATION

L'Assistant d'activation vous signale la réussite de l'activation de Kaspersky Anti-Virus. Il propose également des informations sur la licence : type (commerciale, évaluation, etc.), fin de validité de la licence et nombre d'ordinateurs pouvant utiliser cette licence.

Dans le cas d'activation de l'abonnement, à la place de la date d'expiration de la licence, l'information sur le statut d'abonnement (cf. section "Abonnement pour le renouvellement automatique de la licence" à la page [31](#)) est affichée.

ETAPE 2. SELECTION DU MODE DE PROTECTION

Sélectionnez le mode de protection proposé par Kaspersky Anti-Virus.

Deux choix s'offrent à vous :

- **Automatique.** Lorsque des événements importants surviennent, Kaspersky Anti-Virus exécute automatiquement l'action recommandée par les experts de Kaspersky Lab. Lorsque l'application découvre une menace, il tente de réparer l'objet et si cela est impossible, il le supprime. Les objets suspects sont ignorés sans traitement. Des messages contextuels signalent les événements qui se produisent.
- **Interactif.** Dans ce mode, l'application réagit aux événements conformément à vos choix. Lorsqu'un événement qui requiert votre intervention se manifeste, l'application affiche des notifications (à la page [134](#)) offrant un choix d'actions.

La notification sur la découverte d'une infection active est affichée quel que soit le mode de protection sélectionné.

ETAPE 3. CONFIGURATION DE LA MISE A JOUR DE L'APPLICATION

Cette étape de l'Assistant de configuration de l'application n'apparaît pas si vous avez choisi l'installation express. Les paramètres de l'application configurables à cette étape reçoivent les valeurs par défaut.

La qualité de la protection de votre ordinateur dépend de l'actualité des bases et des modules du logiciel. Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de mise à jour de logiciel et de la programmer :

- **Mise à jour automatique.** Kaspersky Anti-Virus vérifie, selon un intervalle déterminé, si un paquet de mise à jour se trouve dans la source. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Si l'application découvre des nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur. Ce mode est utilisé par défaut.
- **Mise à jour programmée** (l'intervalle varie en fonction des paramètres de la programmation). La mise à jour sera lancée automatiquement selon l'horaire défini. La programmation est configurée dans la fenêtre qui s'ouvre à l'aide du bouton **Configuration**.
- **Mise à jour manuelle.** Vous lancez vous-même la procédure de mise à jour du logiciel.

N'oubliez pas que les bases des signatures des menaces et les modules de l'application qui font partie de l'installation peuvent être dépassées au moment de l'installation de Kaspersky Anti-Virus. C'est la raison pour laquelle nous vous conseillons d'utiliser les mises à jour les plus récentes de Kaspersky Anti-Virus. Il suffit simplement de cliquer sur **Mettre à jour maintenant**. Dans ce cas, le programme recevra les mises à jour requises depuis les serveurs de mise à jour via Internet et les installera sur l'ordinateur.

Si les bases reprises dans la distribution sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Si vous souhaitez accéder aux paramètres de la mise à jour (cf. section "Mise à jour" à la page [87](#)) (sélectionner la ressource d'où la mise à jour sera téléchargée, configurer le lancement de la mise à jour selon les privilèges d'un compte utilisateur en particulier ou activer le service de copie des mises à jour sur une source locale), cliquez sur le bouton **Configuration**.

ETAPE 4. RESTRICTION DE L'ACCES A L'APPLICATION

Cette étape de l'Assistant de configuration de Kaspersky Anti-Virus n'apparaît pas si vous avez choisi l'installation express. Les paramètres de l'application configurables à cette étape reçoivent les valeurs par défaut.

Dans la mesure où l'ordinateur peut être utilisé par plusieurs personnes dont les connaissances en informatique peuvent varier et étant donné que des programmes malveillants pourraient désactiver la protection, vous avez la possibilité de limiter l'accès à Kaspersky Anti-Virus à l'aide d'un mot de passe. Le mot de passe permet de protéger le programme contre les tentatives de désactivation non autorisée de la protection ou contre les modifications des paramètres de Kaspersky Anti-Virus.

Pour activer cette protection, cochez la case ☒ **Activer la protection par mot de passe** et remplissez les champs **Nouveau mot de passe** et **Confirmation du mot de passe**.

Indiquez ensuite l'ampleur de la restriction :

- ☒ **Configuration de l'application** : l'utilisateur est invité à saisir le mot de passe lorsqu'il tente de sauvegarder les modifications des paramètres de Kaspersky Anti-Virus.
- ☒ **Arrêt de l'application** : l'utilisateur doit saisir le mot de passe s'il souhaite arrêter le programme.

ETAPE 5. SELECTION DES MENACES IDENTIFIEES

Cette étape de l'Assistant de configuration de l'application n'apparaît pas si vous avez choisi l'installation express. Les paramètres de l'application configurables à cette étape reçoivent les valeurs par défaut.

Cette étape vous offre la possibilité de sélectionner les catégories de menaces découvertes par Kaspersky Anti-Virus. Kaspersky Anti-Virus découvre toujours les programmes capables de nuire à votre ordinateur. Les virus, les vers et les chevaux de Troie appartiennent à cette catégorie d'applications.

ETAPE 6. FIN DE L'ASSISTANT

La dernière fenêtre de l'Assistant vous signale la fin de l'installation du programme. Pour commencer à utiliser Kaspersky Anti-Virus, assurez-vous que la case ☒ **Lancer Kaspersky Anti-Virus** est cochée puis cliquez sur le bouton **Terminer**.

MISE A JOUR DE L'APPLICATION

La mise à jour de Kaspersky Anti-Virus nécessite une connexion Internet.

Kaspersky Anti-Virus est livré avec des bases qui contiennent les signatures des menaces. Toutefois, il se peut que les bases soient dépassées au moment d'installer Kaspersky Anti-Virus car Kaspersky Lab actualise régulièrement les bases et les modules de l'application.

L'Assistant de configuration de l'application vous permet de sélectionner le mode d'exécution des mises à jour (cf. section "Etape 3. Configuration de la mise à jour de l'application" à la page [28](#)). Kaspersky Anti-Virus vérifie automatiquement la présence des mises à jour sur les serveurs de mises à jour de Kaspersky Lab. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Anti-Virus les télécharge et les installe en arrière plan.

Si les bases reprises dans la distribution sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Pour maintenir la protection de votre ordinateur à jour, il est conseillé d'actualiser Kaspersky Anti-Virus directement après l'installation.

➤ *Pour actualiser manuellement Kaspersky Anti-Virus, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur **Lancer la Mise à jour**.

RECHERCHE DE VIRUS SUR L'ORDINATEUR

Les développeurs d'applications malveillantes déploient beaucoup d'efforts pour masquer leur activité et pour cette raison, il se peut que vous ne remarquiez pas la présence d'applications malveillantes sur votre ordinateur.

Au moment de l'installation de Kaspersky Anti-Virus, l'application exécute automatiquement la tâche **Analyse Rapide** de l'ordinateur. Cette tâche est orientée sur la recherche et la neutralisation de programmes malveillants dans les objets chargés au démarrage du système d'exploitation.

Les experts de Kaspersky Lab conseillent également d'exécuter la tâche **Analyse Complète** de l'ordinateur.

➤ *Pour lancer la tâche d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Cliquez sur le bouton **Lancer l'analyse complète** afin de commencer l'analyse.

RECHERCHE DE VULNERABILITES SUR L'ORDINATEUR

Les paramètres du système d'exploitation reçoivent souvent des valeurs inexactes suite à une activité non sollicitée qui peut résulter d'un échec du système et de l'activité de programmes malveillants. De plus, les applications installées peuvent abriter des vulnérabilités exploitées par les individus mal intentionnés pour nuire à votre ordinateur.

Pour identifier ces problèmes de sécurité et les résoudre, les experts de Kaspersky Lab recommandent de lancer *la tâche de Recherche de Vulnérabilités* (cf. page [82](#)) après l'installation de l'application. Cette tâche consiste à rechercher des vulnérabilités dans les applications ainsi que des anomalies ou des corruptions dans les paramètres du système d'exploitation et du navigateur.

➤ *Pour lancer la tâche de recherche de vulnérabilités, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Cliquez sur le bouton **Ouvrir la fenêtre de recherche de vulnérabilités**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Lancer la recherche de vulnérabilités**.

ADMINISTRATION DE LA LICENCE

Kaspersky Anti-Virus fonctionne grâce à une clé. Le fichier de licence vous est attribué en vertu du code d'activation reçu à l'achat de l'application, et permet de l'utiliser à partir du jour d'activation. Le fichier de licence contient l'information sur la licence : type, durée de validité, nombres d'ordinateurs sur lesquels elle se propage.

Sans le fichier de licence, si la version d'évaluation de Kaspersky Anti-Virus n'a pas été activée, l'application fonctionnera en mode de mise à jour unique. Par la suite, les mises à jour disponibles sur le serveur ne seront pas téléchargées.

Si la version d'évaluation avait été activée, Kaspersky Anti-Virus ne fonctionnera plus une fois que la clé sera arrivée à échéance.

Une fois la clé commerciale expirée, le logiciel continue à fonctionner, si ce n'est qu'il ne sera plus possible de mettre à jour les bases. Vous pourrez toujours analyser l'ordinateur à l'aide de la recherche de virus et utiliser l'Antivirus Fichiers, mais uniquement sur la base des bases de l'application d'actualité à la fin de validité de la licence. Par conséquent, nous ne pouvons pas garantir une protection totale contre les nouveaux virus qui apparaîtraient après l'expiration de la licence.

Afin que l'ordinateur ne soit pas contaminé par de nouveaux virus, nous vous conseillons de prolonger la validité de la licence de Kaspersky Anti-Virus. L'application vous préviendra deux semaines avant l'expiration de la licence. Le message de circonstance apparaîtra à chaque exécution de l'application pendant un certain temps.

L'information sur la licence utilisée est présentée dans la fenêtre **Gestionnaire de licences** : type (commerciale, commerciale avec abonnement, commerciale avec abonnement pour la protection, évaluation), nombre maximum d'ordinateurs sur lesquels elle peut être installée, date d'expiration et nombre de jours restant avant cette date. Les informations relatives à la fin de la validité de la licence n'apparaissent pas pour les licences commerciales avec abonnement ou les licences commerciales avec abonnement pour la protection (cf. section "Abonnement pour le renouvellement automatique de la licence" à la page [31](#)).

Pour lire les termes du contrat de licence pour l'utilisation de l'application, cliquez sur le bouton **Lire le contrat de licence**. Pour supprimer le fichier de licence cliquez sur le bouton  à droite de la licence, en regard du fichier de licence que vous voulez supprimer. Pour activer une nouvelle licence, utilisez le bouton **Activer la nouvelle licence**.

A l'aide des boutons **Acheter une licence (Renouveler la licence)** vous pouvez passer à l'achat (renouvellement) de la licence dans la boutique en ligne de Kaspersky Lab.

Kaspersky Lab organise à intervalles réguliers des actions qui permettent de renouveler la licence d'utilisation de ses logiciels en bénéficiant de remises considérables. Soyez à l'affût de ces actions sur le site de Kaspersky Lab dans la rubrique **Produits → Actions et offres spéciales**.

ABONNEMENT POUR LE RENOUVELLEMENT AUTOMATIQUE DE LA LICENCE

L'abonnement permet de renouveler automatiquement la durée de validité de la licence. L'activation de l'abonnement requiert un code d'activation délivré par la boutique en ligne lors de l'achat de Kaspersky Anti-Virus.

Si au moment d'activer l'abonnement vous aviez déjà activé une licence avec une validité limitée, elle sera remplacée par une licence avec abonnement. Si vous ne souhaitez pas utiliser le service d'abonnement, vous devrez contacter le magasin en ligne où vous avez acheté Kaspersky Anti-Virus.

L'abonnement peut avoir un des états suivants :

- **Définition en cours.** La demande d'activation de l'abonnement n'a pas encore été traitée (le traitement des requêtes sur le serveur requiert un certain temps). Kaspersky Anti-Virus fonctionne en mode plein-fonctionnel. Si l'abonnement n'a pas été traité à la fin d'un délai déterminé, vous recevrez un message indiquant que l'actualisation de l'abonnement n'a pas été réalisée. Les bases de l'application ne seront plus actualisées (pour les licences avec abonnement) et l'ordinateur ne sera plus protégé (pour les licences avec abonnement pour la protection).
- **Activé.** L'abonnement a été activé pour une durée indéterminée ou non (la date de fin de validité est alors précisée).
- **Renouvelé.** L'abonnement a été renouvelé pour une durée indéterminée ou non.
- **Erreur.** Une erreur s'est produite lors de l'actualisation de l'état de l'abonnement.

- *Expiré. La période de grâce est en cours.* La durée de validité de l'abonnement ou le délai pour l'actualisation de l'abonnement est écoulé. Si le délai pour l'actualisation est écoulé, actualisez l'état de l'abonnement manuellement. Si la durée de validité de l'abonnement est écoulée, vous pouvez le renouveler en contactant le magasin en ligne où vous avez acheté Kaspersky Anti-Virus. Avant de pouvoir utiliser un autre code d'activation, il faut d'abord supprimer le fichier de licence pour l'abonnement utilisé.
- *Expiré. La période de grâce est écoulée.* La durée de validité de l'abonnement ou la période de grâce pour le renouvellement de celui-ci est écoulée. Contactez le fournisseur de l'abonnement pour obtenir un nouvel abonnement ou renouveler l'abonnement actuel.
- *Refus d'abonnement.* Vous avez refusé d'utiliser l'abonnement pour le renouvellement automatique de la licence.
- *Actualisation requise.* L'état de l'abonnement n'a pas été actualisé à temps pour une raison quelconque. Cliquez sur le bouton **Renouveler l'état de l'abonnement** pour actualiser l'état de l'abonnement.
- *Suspendu.* L'abonnement pour le renouvellement automatique de la licence a été suspendu.
- *Renouvelé.* L'abonnement a été renouvelé.

Si la durée de validité de l'abonnement est écoulée ainsi que la période de grâce durant laquelle le renouvellement est possible (état *Expiré*), Kaspersky Anti-Virus vous le signale et cesse de tenter de renouveler automatiquement la licence. Dans le cas des licences avec abonnement, les fonctions de l'application sont préservées à l'exception de la mise à jour des bases de l'application. Dans le cas d'une licence avec abonnement pour la protection, les bases de l'application ne seront plus actualisées, l'ordinateur ne sera plus protégé et les analyses ne seront plus exécutées.

Si la licence n'a pas été renouvelée pour une raison quelconque (état *Actualisation requise*) à temps (par exemple, l'ordinateur n'était pas allumé pendant la période où le renouvellement de la licence était possible), vous pouvez actualiser son état manuellement. Avant le renouvellement de l'abonnement, Kaspersky Anti-Virus n'actualise plus les bases de l'application (pour les licences avec abonnement) et cesse de protéger l'ordinateur et de lancer l'analyse (pour les licences commerciales avec abonnement pour la protection).

En cas d'utilisation de l'abonnement, vous ne pouvez pas utiliser un autre code d'activation pour prolonger la durée de validité de la licence. Ceci sera possible uniquement à l'échéance de l'abonnement (état *A expiré*). Pour renouveler la durée de validité de l'application, vous bénéficierez d'une période de remise au cours de laquelle les fonctions de l'application seront préservées.

N'oubliez pas que si vous devez réinstaller l'application et que vous utilisez l'abonnement, vous devrez actualiser à nouveau le logiciel manuellement à l'aide du code d'activation reçu à l'achat de l'application.

La liste des actions possibles avec l'abonnement varie en fonction du fournisseur. Il est possible également qu'aucune période de grâce ne soit accordée pour le renouvellement de l'abonnement.

PARTICIPATION AU KASPERSKY SECURITY NETWORK

Chaque jour dans le monde, une multitude de nouveaux virus apparaissent. Pour accélérer la collecte de statistiques sur le type de nouvelles menaces, sur leur source et sur les moyens de les neutraliser, Kaspersky Lab vous propose de participer au Kaspersky Security Network.

L'utilisation de Kaspersky Security Network permet d'envoyer les informations suivantes à Kaspersky Lab :

- L'identificateur unique attribué à votre ordinateur par Kaspersky Anti-Virus. Cet identificateur définit les paramètres matériels de l'ordinateur et ne contient aucune information personnelle.
- Les informations relatives aux menaces découvertes par les composants du programme. Le contenu de ces informations dépend du type de menace identifiée.
- Informations relatives au système : version du système d'exploitation, mises à jour installées, services et pilotes téléchargés, version des navigateurs et des clients de messagerie, modules externes des navigateurs, numéro de la version de l'application de Kaspersky Lab installée.

Kaspersky Security Network collecte également des statistiques très diverses qui contiennent, entre autres, les informations sur les éléments suivants :

- les fichiers exécutables et les applications signées téléchargées sur l'ordinateur ;
- les applications exécutées sur l'ordinateur.

L'envoi des informations statistiques se produit à la fin de la mise à jour de l'application.

Kaspersky Lab garantit qu'aucune donnée personnelle n'est recueillie ni envoyée dans le cadre de Kaspersky Security Network.

➡ Pour configurer les paramètres de l'envoi de statistiques, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Retour d'informations**.
3. Cochez la case ☒ **J'accepte de rejoindre le Kaspersky Security Network** pour confirmer votre participation au Kaspersky Security Network.

ADMINISTRATION DE LA SECURITE

La présence d'un problème dans la protection de l'ordinateur est signalée par l'état de la protection de l'ordinateur (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page [39](#)) : l'icône de l'état de la protection et du panneau sur lequel elle se trouve change de couleur. Il est conseillé de résoudre les problèmes du système de protection dès qu'ils se manifestent.



Illustration 1: Etat actuel de la protection de l'ordinateur

Vous pouvez consulter la liste des problèmes, leur description et les solutions éventuelles sous l'onglet **Etat** (cf. ill. ci-dessous) dont la sélection s'opère si vous cliquez sur l'icône de l'état ou du panneau sur lequel elle est située (cf. ill. ci-dessus).

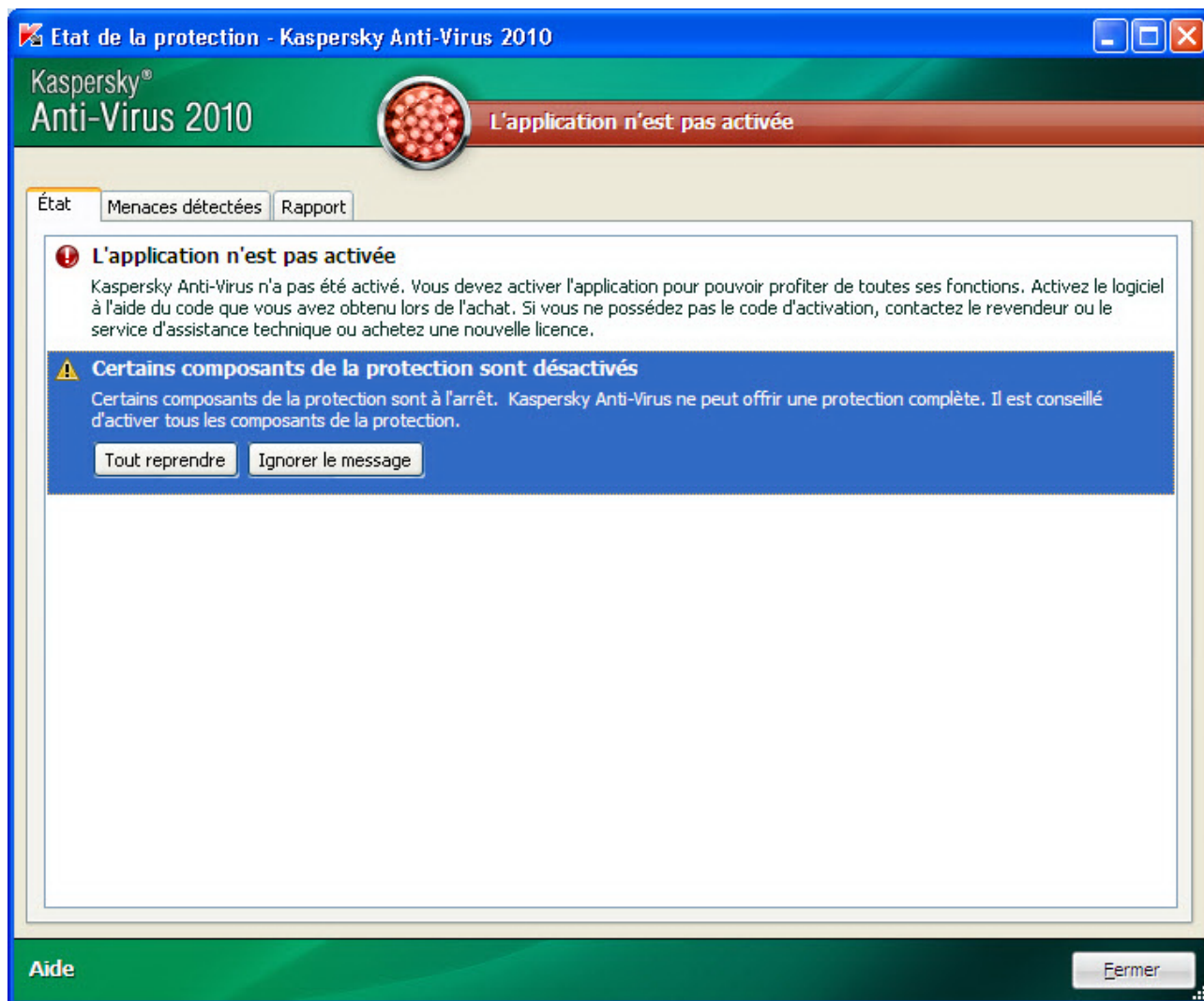


Illustration 2 : Résolution des problèmes de sécurité

Vous pouvez consulter la liste des problèmes rencontrés. Les problèmes sont classés par ordre de gravité : viennent d'abord les problèmes les plus graves, à savoir ceux dont l'état est marqué par une icône rouge ; ensuite viennent les problèmes moins importants (icône d'état jaune) et en dernier lieu, nous avons les messages informatifs. Chaque problème est accompagné d'une description et les actions suivantes sont proposées :

- **Résolution immédiate.** Grâce aux boutons correspondants, vous pouvez passer à la suppression directe du problème, ce qui est l'action recommandée.
- **Reporter la suppression.** Si pour une raison quelconque il est impossible de résoudre les problèmes sur le champ, on peut reporter l'action et y revenir plus tard. Pour ce faire, cliquez sur le bouton **Ignorer le message**.

Sachez toutefois que cette possibilité n'est pas reprise pour les problèmes graves. Il s'agit par exemple de la présence d'objets malveillants non neutralisés, de l'échec d'un ou de plusieurs composants ou de la corruption de fichiers de l'application.

Pour que des messages dissimulés soient à nouveau visibles dans la liste générale, cochez la case ☒ **Afficher les messages dissimulés**.

ÉTAT DE LA PROTECTION

Le travail des composants de Kaspersky Anti-Virus ou des tâches d'analyse est consigné dans une rubrique contenant des informations de synthèse sur l'état de la protection de l'ordinateur. Vous pouvez voir ici le nombre d'objets dangereux ou suspects découverts pendant l'utilisation de l'application ainsi que le nombre d'objets réparés, supprimés ou placés en quarantaine.

La découverte d'objets malveillants est indiquée par l'état de la protection de l'ordinateur (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page 39) via un changement de couleur de l'icône et du panneau sur lequel elle apparaît. En cas de découverte d'objet malveillant, l'icône et le panneau deviennent rouge. Dans ce cas, il faut supprimer immédiatement toutes les menaces.

➤ *Pour connaître l'état de la protection de l'ordinateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapport**.

➤ *Pour supprimer les problèmes de la protection de l'ordinateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapport**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Etat**, exécutez les actions requises. Pour que des messages dissimulés soient à nouveau visibles dans la liste générale, cochez la case ☒ **Afficher les messages ignorés**.

➤ *Pour exécuter une action sur l'objet trouvé, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapport**.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces détectées**, sélectionnez l'objet souhaité et cliquez sur celui-ci avec le bouton droit de la souris dans la liste des objets.
4. Dans le menu contextuel qui s'ouvre, sélectionnez l'action requise.

➤ *Pour voir le rapport sur le fonctionnement des composants de la protection, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Rapport**.
3. Dans la fenêtre qui s'ouvre sélectionnez l'onglet **Rapport**.

SUSPENSION DE LA PROTECTION

La suspension de la protection signifie la désactivation de tous ses composants pour un certain temps.

Cette action suspend le fonctionnement de tous les composants de la protection en temps. Les éléments suivants permettent de confirmer la désactivation :

- l'icône de l'application dans la zone de notification de la barre des tâches est en grise ;
- couleur rouge de l'icône d'état et du panneau de la fenêtre principale de Kaspersky Anti-Virus.

Si des connexions de réseau étaient ouvertes au moment de la suspension de l'application, un message sur l'interruption de ces connexions sera affiché.

➡ *Pour suspendre la protection de l'ordinateur, procédez comme suit :*

1. Dans le menu contextuel (cf. section "Menu contextuel" à la page [38](#)) de l'application sélectionnez **Suspension de la protection**.
2. Dans la fenêtre **Suspension de la protection** qui s'ouvre, sélectionnez la durée à l'issue de laquelle la protection sera à nouveau activée :
 - **Suspendre pendant <intervalle>** : la protection sera restaurée à l'issue de l'intervalle désigné. Pour sélectionner la valeur, utilisez la liste déroulante.
 - **Suspendre jusqu'au redémarrage** – la protection sera activée après le redémarrage de l'application ou du système (pour autant que le mode de lancement de Kaspersky Anti-Virus au démarrage de l'ordinateur ait été activé).
 - **Suspendre** : la protection sera réactivée uniquement lorsque vous le déciderez. Pour activer la protection, cliquez sur le point **Lancement de la protection** dans le menu contextuel de l'application.

INTERFACE DE L'APPLICATION

L'interface de Kaspersky Anti-Virus est simple et conviviale. Ce chapitre aborde en détail les principaux éléments de l'interface.

Kaspersky Anti-Virus possède des modules externes (plug-in) qui peuvent être intégrés à Microsoft Office Outlook, The Bat!, Microsoft Internet Explorer et Microsoft Windows Explorer. Les modules externes élargissent les possibilités des programmes cités et permettent de configurer, depuis leur interface, les paramètres des composants de l'application.

DANS CETTE SECTION

Icône dans la zone de notification.....	37
Menu contextuel	38
Fenêtre principale de Kaspersky Anti-Virus.....	39
Notifications.....	41
Fenêtre de configuration des paramètres de l'application	41

ICONE DANS LA ZONE DE NOTIFICATION

L'icône de l'application apparaît dans la zone de notification de la barre des tâches de Microsoft Windows directement après son installation.

L'icône indique le fonctionnement de l'application. Elle représente l'état de la protection et montre également plusieurs actions fondamentales exécutées par l'application.

Si l'icône est active  (en couleur), cela signifie que la protection est complètement activée ou que certains de ses composants fonctionnent. Si l'icône est inactive  (noir et blanc), cela signifie que tous les composants de la protection sont désactivés.

L'icône de l'application varie en fonction de l'opération exécutée :



– analyse d'un message électronique en cours ;



– mise à jour des bases et des modules de l'application en cours ;



– redémarrage de l'ordinateur requis pour appliquer les mises à jour ;



– échec du fonctionnement d'un composant quelconque de l'application.

L'icône permet également d'accéder aux éléments fondamentaux de l'interface de l'application que sont le menu contextuel (cf. section "Menu contextuel" à la page [38](#)) et la fenêtre principale (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page [39](#)).

Pour ouvrir le menu contextuel, cliquez avec le bouton droit de la souris sur l'icône de l'application.

Pour ouvrir la fenêtre principale de Kaspersky Anti-Virus, cliquez avec le bouton gauche de la souris sur l'icône de l'application.

L'icône  apparaît dans la barre des tâches de Microsoft Windows lorsque des infos sont émises par Kaspersky Lab. Cliquez deux fois sur l'icône pour prendre connaissance du texte des informations.

MENU CONTEXTUEL

Le menu contextuel permet d'exécuter toutes les tâches principales liées à la protection.

Le menu de l'application contient les points suivants :

- **Mise à jour** : lance la mise à jour des bases et des modules de l'application et l'installe sur l'ordinateur.
- **Analyse complète** : lance l'analyse complète de l'ordinateur afin d'identifier la présence éventuelle d'objets malveillants. Les objets de tous les disques, y compris sur les disques amovibles, seront analysés.
- **Recherche de virus** : passe à la sélection d'objets et au lancement de la recherche de virus. La liste contient par défaut une multitude d'objets tels que le répertoire **Mes documents** et les boîtes aux lettres. Vous pouvez enrichir la liste, sélectionner des objets à analyser et lancer la recherche de virus.
- **Clavier virtuel** : accès au clavier virtuel.
- **Kaspersky Anti-Virus** : ouvre la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page [39](#)).
- **Configuration** : permet d'afficher et de configurer les paramètres de fonctionnement de l'application.
- **Activation** : passe à l'activation de Kaspersky Anti-Virus. Pour bénéficier des privilèges accordés aux utilisateurs enregistrés, vous devez impérativement activer votre copie de l'application. Ce point du menu est visible uniquement si l'application n'a pas été activée.
- **A propos du programme** : ouvre une boîte de dialogue contenant des informations sur l'application.
- **Suspension de la protection / Lancement de la protection** : suspension temporaire / activation des composants de la protection en temps réel. Ce point du menu n'a aucune influence sur la mise à jour de l'application, ni sur l'exécution de la recherche de virus.
- **Terminer** : arrêt du fonctionnement de Kaspersky Anti-Virus (si vous choisissez cette option, l'application sera déchargée de la mémoire vive de l'ordinateur).



Illustration 3: Menu contextuel

Si une tâche quelconque de recherche de virus est lancée quand vous ouvrez le menu contextuel, son nom apparaît dans le menu contextuel accompagné de la progression en pour cent. Après avoir sélectionné une tâche, vous pouvez passer à la fenêtre principale avec le rapport contenant les résultats détaillés de l'exécution.

FENETRE PRINCIPALE DE KASPERSKY ANTI-VIRUS

La fenêtre principale de l'application est scindée en trois parties :

- La partie supérieure reprend une évaluation globale de l'état de la protection de votre ordinateur.



Illustration 4: Etat actuel de la protection de l'ordinateur

Il existe trois états possibles pour la protection. Chacun d'entre eux est associé à une couleur particulière, comme pour les feux signalisation. Le vert indique que la protection de l'ordinateur est assurée au niveau requis. Le jaune et le rouge signalent la présence de menaces de divers types pour la sécurité. Les menaces sont non seulement les applications malveillantes, mais également les bases de l'application dépassée, certains composants désactivés, les paramètres minimes de fonctionnement de l'application, etc.

Il faut remédier aux menaces pour la sécurité au fur et à mesure qu'elles se présentent. Pour en obtenir des informations détaillées et de les supprimer rapidement, passez à l'Assistant d'administration de la sécurité, cliquez sur l'icône de l'état ou du panneau sur lequel elle est située (cf. ill. ci-dessus).

- La partie gauche de la fenêtre permet d'accéder rapidement à n'importe quelle fonction de l'application, au lancement de la recherche de virus ou de la mise à jour, etc.



Illustration 5: Partie gauche de la fenêtre principale

- La partie droite de la fenêtre contient des informations relatives à la fonction de l'application choisie dans la partie gauche. Vous pouvez configurer les paramètres de la fonction, utiliser des outils pour exécuter les recherches de virus et la récupération des mises à jour, etc.



Illustration 6: Partie droite de la fenêtre principale

Vous pouvez également cliquer sur les boutons et les liens suivants :

- **Configuration** : ouvre la fenêtre de configuration des paramètres de l'application (cf. section "Configuration des paramètres de l'application" à la page 94).
- **Menaces en quarantaine** : passe à la manipulation des objets placés en quarantaine.
- **Rapport** : passe à la liste des événements survenus pendant le fonctionnement de l'application.
- **Aide** : accès à l'aide de Kaspersky Anti-Virus.
- **Mon Espace Personnel** : ouvre l'espace personnel de l'utilisateur sur le site du service d'assistance technique.
- **Assistance technique** : ouvre la fenêtre contenant les informations relatives au système et les liens vers les sources d'informations de Kaspersky Lab (site du service d'assistance technique, forum).
- **Licence** : passe à l'activation de Kaspersky Anti-Virus et au renouvellement de la licence.

Vous pouvez également modifier l'apparence de l'application en créant et en utilisant des éléments graphiques particuliers et la palette de couleurs.

NOTIFICATIONS

Lorsqu'un événement survient durant l'utilisation de Kaspersky Anti-Virus, des notifications apparaissent à l'écran sous la forme de messages contextuels au-dessus de l'icône de l'application dans la barre des tâches de Microsoft Windows.

En fonction du degré d'importance de l'événement (au niveau de la sécurité de l'ordinateur), les notifications peuvent être de divers type :

- **Alertes.** Un événement critique est survenu, par exemple : découverte d'un virus ou d'une activité dangereuse dans le système. Il faut immédiatement décider de la suite des événements. Les notifications de ce type apparaissent en rouge.
- **Attention.** Un événement qui présente un risque potentiel s'est produit, par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système. Vous devez décider du danger que représente cet événement. Les notifications de ce type apparaissent en jaune.
- **Informations.** Ce message vous signale un événement qui n'est pas critique. Les messages d'informations sont en vert.

VOIR EGALEMENT

Notifications..... [134](#)

FENETRE DE CONFIGURATION DES PARAMETRES DE L'APPLICATION

La fenêtre de configuration des paramètres de Kaspersky Anti-Virus peut être ouverte de la fenêtre principale (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page [39](#)) ou du menu contextuel (cf. section "Menu contextuel" à la page [38](#)). Pour ce faire, cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre ou choisissez l'option du même nom dans le menu contextuel de l'application.

La fenêtre de configuration contient deux parties :

- la partie gauche permet d'accéder aux fonctions de Kaspersky Anti-Virus, aux tâches de recherche de virus, à la mise à jour, etc. ;
- la partie droite reprend une énumération des paramètres du composant, de la tâche, etc. sélectionnés dans la partie gauche.

PROTECTION DU SYSTEME DE FICHIERS DE L'ORDINATEUR

L'*Antivirus Fichiers* permet d'éviter l'infection du système de fichiers de l'ordinateur. Ce composant est lancé en même temps que le système d'exploitation, demeure en permanence dans la mémoire vive de l'ordinateur et analyse tous les programmes ou fichiers que vous ouvrez, enregistrez ou exécutez.

Par défaut, l'Antivirus Fichiers analyse uniquement les nouveaux fichiers et les fichiers modifiés. L'analyse des fichiers se déroule selon un ensemble défini de paramètres désigné sous le concept de niveau de protection. Quand Antivirus Fichiers découvre une menace, il exécute l'action définie.

Le niveau de protection des fichiers et de la mémoire est défini par les groupes de paramètres suivants qui :

- définissent la zone protégée ;
- définissent la méthode d'analyse utilisée ;
- définissent l'analyse des fichiers composés (y compris les fichiers composés de grande taille) ;
- définissent le mode d'analyse ;
- permettent de suspendre le fonctionnement du composant selon la programmation ou pendant l'utilisation d'applications définies.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Fichiers. Dans la majorité des cas, la modification du niveau de protection suffit. Vous pouvez restaurer les paramètres de fonctionnement par défaut de l'Antivirus Fichiers. Pour ce faire, sélectionnez un des niveaux de protection.

➡ Afin de modifier les paramètres de fonctionnement de l'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Modifiez les paramètres du composant selon vos besoins.

DANS CETTE SECTION

Algorithme de fonctionnement du composant.....	43
Modification du niveau de protection des fichiers et de la mémoire	44
Modification de l'action à réaliser sur les objets identifiés	44
Constitution de la zone de protection	45
Utilisation de l'analyse heuristique	46
Optimisation de l'analyse.....	46
Analyse des fichiers composés.....	47
Analyse des objets composés de grande taille	47
Modification du mode d'analyse.....	48
Technologie d'analyse.....	48
Suspension du composant : programmation	49
Suspension du composant : composition de la liste des applications	50
Restauration des paramètres de protection par défaut	51

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

L'*Antivirus Fichiers* est lancé en même temps que le système d'exploitation, demeure en permanence dans la mémoire vive de l'ordinateur et analyse tous les programmes ou fichiers que vous ouvrez, enregistrez ou exécutez.

Par défaut, l'*Antivirus Fichiers* analyse uniquement les nouveaux fichiers ou les fichiers modifiés, c.-à-d. les fichiers qui ont été ajoutés, ou modifiés depuis la dernière fois qu'ils ont été sollicités. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. Le composant intercepte les requêtes de l'utilisateur ou d'un programme quelconque adressé à chaque fichier.
2. L'*Antivirus Fichiers* recherche des informations sur le fichier intercepté dans les bases iChecker et iSwift et sur la base des informations obtenues, il décide s'il faut analyser ou non le fichier.

Les actions suivantes sont réalisées durant l'analyse :

1. Le fichier est soumis à la recherche d'éventuels virus. L'identification des objets malveillants s'opère à l'aide des bases de Kaspersky Anti-Virus. Les bases contiennent la définition de tous les programmes malveillants, menaces et attaques de réseau connus à ce jour et leur mode de neutralisation.
2. Selon les résultats de l'analyse, Kaspersky Anti-Virus peut adopter les comportements suivants :
 - a. Si le fichier contient un code malveillant, l'*Antivirus Fichiers* le bloque, place une copie dans le dossier de sauvegarde et tente de le réparer. Si la réparation réussit, l'utilisateur peut utiliser le fichier. Dans le cas contraire, le fichier est supprimé.
 - b. Si le fichier contient un code semblable à un code malveillant et que ce verdict ne peut pas être garanti à 100%, le fichier est réparé et placé dans un répertoire spécial : la quarantaine.
 - c. Si aucun code malveillant n'a été découvert dans le fichier, le destinataire pourra l'utiliser immédiatement.

Quand l'application découvre un objet infecté ou potentiellement infecté, elle vous le signale. Suite à la découverte d'un objet infecté ou potentiellement infecté, un message interrogeant l'utilisateur sur la suite des opérations s'affichera. Vous aurez le choix entre les options suivantes :

- placer la menace en quarantaine en vue d'une analyse et d'un traitement ultérieur à l'aide de bases actualisées ;
- supprimer l'objet ;
- ignorer l'objet si vous êtes absolument convaincu qu'il n'est pas malveillant.

MODIFICATION DU NIVEAU DE PROTECTION DES FICHIERS ET DE LA MEMOIRE

Le niveau de protection désigne un ensemble prédéfini de paramètres de l'Antivirus Fichiers. Les experts de Kaspersky Lab ont configuré trois niveaux de protection. La sélection du niveau de protection est déterminée par l'utilisateur en fonction des conditions de travail et la situation en vigueur. Vous avez le choix entre l'un des niveaux de protection suivants :

- **Elevé.** Choisissez ce niveau si vous pensez que la probabilité d'une infection de votre ordinateur est très élevée.
- **Recommandé.** Ce niveau assure l'équilibre optimal entre les performances et la sécurité et convient à la majorité des cas.
- **Bas.** Si vous travaillez dans un milieu pourvu d'une protection (par exemple, dans un réseau d'entreprise avec une sécurité centralisée), le niveau Bas vous conviendra. Ce niveau peut également être choisi en cas d'utilisation d'applications gourmandes en ressources.

Avant d'activer le niveau de protection bas pour les fichiers, il est conseillé de lancer une analyse complète de l'ordinateur au niveau de protection élevé.

Si aucun des niveaux proposés ne répond pas à vos besoins, vous pouvez configurer les paramètres de fonctionnement (cf. section "Protection du système de fichiers de l'ordinateur" à la page [42](#)) de l'Antivirus Fichiers. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut du composant, sélectionnez un des niveaux proposés.

➡ Pour modifier le niveau proposé de protection des fichiers et de la mémoire, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Définissez le niveau de protection requis pour le composant sélectionné.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS IDENTIFIES

Suite à l'analyse, l'Antivirus Fichiers attribue un des états suivants aux objets découverts :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*) ;
- *Probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le fichier contient une séquence de code d'un virus inconnu ou le code modifié d'un virus connu.

Kaspersky Anti-Virus vous avertira s'il découvre des objets infectés ou potentiellement infectés suite à l'analyse. Vous devrez réagir à la menace en sélectionnant une action à exécuter sur l'objet. En cas de sélection de l'option **Confirmer l'action** pour les actions à réaliser sur l'objet identifié, le comportement de Kaspersky Anti-Virus sera le comportement par défaut. Vous pouvez modifier l'action. Par exemple, si vous êtes convaincu chaque objet découvert doit être soumis à une tentative de réparation et que vous ne souhaitez pas à chaque fois choisir l'option **Réparer** au moment de recevoir la notification sur la découverte d'un objet infecté ou suspect, vous pourrez choisir l'option **Exécuter l'action. Réparer**.

Avant de réparer ou de supprimer un objet, Kaspersky Anti-Virus crée une copie de sauvegarde au cas où la restauration de l'objet serait requise ou si la possibilité de le réparer se présentait.

Si vous travaillez en mode automatique (cf. section "Étape. Sélection du mode de protection" à la page 28), Kaspersky Anti-Virus appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants l'action sera **Réparer. Supprimer si la réparation est impossible et pour les objets suspects : Ignorer**.

➡ Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Désignez l'action requise pour le composant sélectionné.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone de protection fait référence non seulement à l'emplacement où se trouvent les objets analysés mais également au type de fichiers à analyser. Kaspersky Anti-Virus analyse par défaut uniquement les fichiers qui pourraient être infectés et qui sont exécutés sur tous les disques durs, les disques amovibles et les disques de réseau.

Vous pouvez étendre ou restreindre la zone d'analyse en ajoutant ou en supprimant des objets à analyser ou en modifiant le type de fichiers à analyser. Par exemple, vous souhaitez analyser uniquement les fichiers exe lancés depuis les disques de réseau. Il faut toutefois être certain de ne pas exposer l'ordinateur à un risque d'infection lors de la définition de la zone d'analyse.

Lors de la sélection du type de fichiers, il convient de garder à l'esprit les éléments suivants :

- La probabilité d'insertion d'un code malveillant et de son activation dans les fichiers de certains formats (par exemple, *txt*) est assez faible. Il existe également des formats qui contiennent ou qui pourraient contenir un code exécutable (*exe*, *dll*, *doc*). Le risque d'intrusion et d'activation ultérieure d'un code malveillant dans ces fichiers est assez élevé.
- La personne mal intentionnée peut envoyer un virus sur votre ordinateur dans un fichier dont l'extension est *txt* alors qu'il s'agit en fait d'un fichier exécutable renommé en fichier *txt*. Si vous sélectionnez l'option  **Fichiers analysés selon l'extension**, ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option  **Fichiers analysés selon le format**, l'Antivirus Fichiers ignorera l'extension, analysera l'en-tête du fichier et découvrira qu'il s'agit d'un fichier *exe*. Le fichier sera alors soumis à une analyse antivirus.

➡ Afin de modifier la liste des objets à analyser, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans la section **Zone d'analyse** cliquez sur le lien **Ajouter**.

5. Dans la fenêtre **Sélection de l'objet à analyser**, sélectionnez l'objet et cliquez sur le bouton **Ajouter**.
6. Après avoir ajouté tous les fichiers requis, cliquez sur **OK** dans la fenêtre **Sélection de l'objet à analyser**.
7. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

➡ *Afin de modifier la priorité de la règle, exécutez l'opération suivante :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le bloc **Type de fichiers** sélectionnez le paramètre requis.

UTILISATION DE L'ANALYSE HEURISTIQUE

Par défaut, l'analyse est réalisée à l'aide des bases qui contiennent une description des menaces connues et les méthodes de réparation. Kaspersky Anti-Virus compare l'objet décelé aux enregistrements des bases, ce qui vous permet d'obtenir une réponse univoque sur la nature indésirable de l'objet analysé et sur la catégorie de programmes malveillants à laquelle il appartient. C'est ce qu'on appelle *l'analyse sur la base de signature* et cette méthode est toujours utilisée par défaut.

Entre temps, chaque jour voit l'apparition de nouveaux objets malveillants dont les enregistrements ne figurent pas encore dans les bases. L'analyse heuristique permet de découvrir ces objets. La méthode repose sur l'analyse de l'activité de l'objet dans le système. Si cet activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Ainsi, les nouvelles menaces seront identifiées avant que leur activité ne soit remarquée par les spécialistes des virus.

En cas de découverte d'un objet malveillant, vous recevrez un message avec une requête sur la marche à suivre.

Vous pouvez définir également le niveau de détail de l'analyse. Le niveau définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de détails est élevé, plus l'analyse utilise de ressources et plus longtemps elle dure.

➡ *Pour commencer à utiliser l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans la section **Méthodes d'analyse**, cochez la case ☒ **Analyse heuristique** et définissez le niveau de détail de l'analyse en dessous.

OPTIMISATION DE L'ANALYSE

Pour réduire la durée de l'analyse et accélérer le fonctionnement de Kaspersky Anti-Virus, vous pouvez analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode de travail touchera aussi bien les fichiers simples que les fichiers composés.

➤ *Afin d'analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans la section **Optimisation de l'analyse** cochez la case ☒ **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés (archives, bases de données, etc.) est une pratique très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Les paquets d'installation et les fichiers qui contiennent des objets OLE sont exécutés à l'ouverture, ce qui les rend plus dangereux que des archives. Vous pouvez protéger votre ordinateur contre l'exécution d'un code malveillant et réduire en même temps la durée de l'analyse en désactivant l'analyse des archives et en activant l'analyse des fichiers de type donné.

Par défaut, Kaspersky Anti-Virus analyse uniquement les objets OLE joints.

➤ *Pour modifier la liste des fichiers composés à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Performance** dans le groupe **Analyse des fichiers composés**, cochez les cases ☒ en regard des types d'objets composés qui seront analysés par l'application.

ANALYSE DES OBJETS COMPOSES DE GRANDE TAILLE

Lors de l'analyse des fichiers composés de grande taille, le décompactage préalable peut prendre un certain temps. La durée peut être réduite si l'analyse des fichiers est réalisée en arrière-plan. Si un objet malveillant est découvert pendant l'utilisation de ces fichiers, Kaspersky Anti-Virus vous le signale.

Pour réduire la durée du temps d'attente avant de pouvoir accéder à des fichiers composés, il est possible de désactiver le décompactage de fichiers dont la taille est supérieure à la valeur définie. L'analyse des fichiers aura toujours lieu au moment de l'extraction de l'archive.

➤ *Pour que Kaspersky Anti-Virus décompacte les fichiers de grande taille en arrière-plan, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans le groupe **Analyse des fichiers composés** cliquez sur le bouton **Avancé**.

5. Dans la fenêtre **Fichiers composés** cochez la case ☒ **Décompacter les fichiers composés en arrière-plan** et définissez la taille minimale du fichier dans le champ en dessous.

➡ *Afin que Kaspersky Anti-Virus ne décompacte pas les fichiers de grande taille, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans le groupe **Analyse des fichiers composés** cliquez sur le bouton **Avancé**.
5. Dans la fenêtre **Fichiers composés** cochez la case ☒ **Ne pas décompacter les fichiers composés de grande taille** et définissez la taille maximale du fichier dans le champ du dessous.

MODIFICATION DU MODE D'ANALYSE

Le mode d'analyse désigne la condition de déclenchement d'Antivirus Fichiers. Kaspersky Anti-Virus utilise par défaut le mode intelligent dans lequel la décision d'analyser un objet est prise sur la base des opérations exécutées avec celui-ci. Par exemple, dans le cas d'un fichier Microsoft Office, Kaspersky Anti-Virus analyse le fichier à la première ouverture et à la dernière fermeture. Toutes les opérations intermédiaires sur le fichier sont exclues de l'analyse.

Vous pouvez modifier le mode d'analyse des objets. La sélection du mode dépend du type de fichiers que vous manipulez le plus souvent.

➡ *Afin de modifier la mode d'analyse des objets, exécutez l'opération suivante :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Mode d'analyse** sélectionnez le mode requis.

TECHNOLOGIE D'ANALYSE

Vous pouvez indiquer également la technologie qui sera utilisée par l'Antivirus Fichiers :

- **iChecker.** Cette technologie permet d'accélérer l'analyse en excluant certains objets. Les objets sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date d'édition des bases de Kaspersky Anti-Virus, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse.

Admettons que vous possédiez une archive qui a reçu l'état *sain* après l'analyse. Lors de l'analyse suivante, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases, l'archive sera analysée à nouveau.

La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux objets dont la structure est connue de l'application (exemple : fichiers *exe, dll, lnk, ttf, inf, sys, com, chm, zip* ou *rar*).

- **iSwift.** Cette technologie est un développement de la technologie iChecker pour les ordinateurs dotés d'un système de fichiers NTFS. Il existe certaines restrictions à la technologie iSwift : elle s'applique à l'emplacement

particulier d'un fichier dans le système de fichiers et elle ne s'applique qu'aux objets des systèmes de fichiers NTFS.

➡ Afin de modifier la technologie d'analyse des objets, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Technologies d'analyse** sélectionnez les paramètres requis.

SUSPENSION DU COMPOSANT : PROGRAMMATION

Lorsque vous exécutez des tâches qui requièrent beaucoup de ressources du système d'exploitation, vous pouvez suspendre temporairement l'Antivirus Fichiers. Pour réduire la charge et permettre l'accès rapide aux objets, vous pouvez configurer la suspension du composant pendant un certain temps.

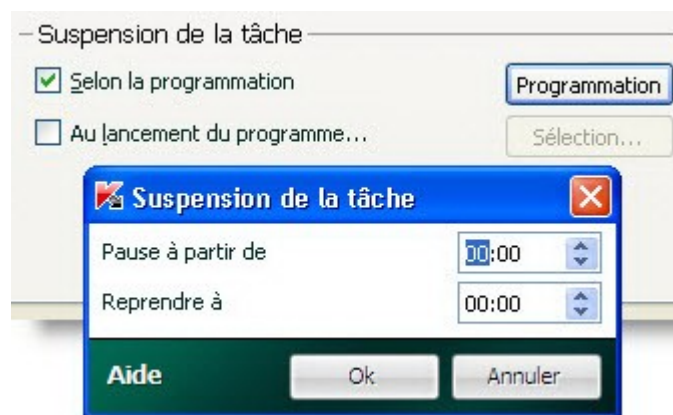


Illustration 7: Planification

➡ Pour programmer la suspension du composant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Suspension de la tâche** cochez la case ☒ **Selon la programmation** puis cliquez sur **Programmation**.
5. Dans la fenêtre **Suspension de la tâche**, indiquez l'heure (au format HH:MM) pendant laquelle la protection sera suspendue (champs **Pause à partir de** et **Reprendre à**).

SUSPENSION DU COMPOSANT : COMPOSITION DE LA LISTE DES APPLICATIONS

Lorsque vous exécutez des tâches qui requièrent beaucoup de ressources du système d'exploitation, vous pouvez suspendre temporairement l'Antivirus Fichiers. Pour réduire la charge et permettre l'accès rapide aux objets, vous pouvez configurer la suspension du composant lors de l'utilisation de certains programmes.

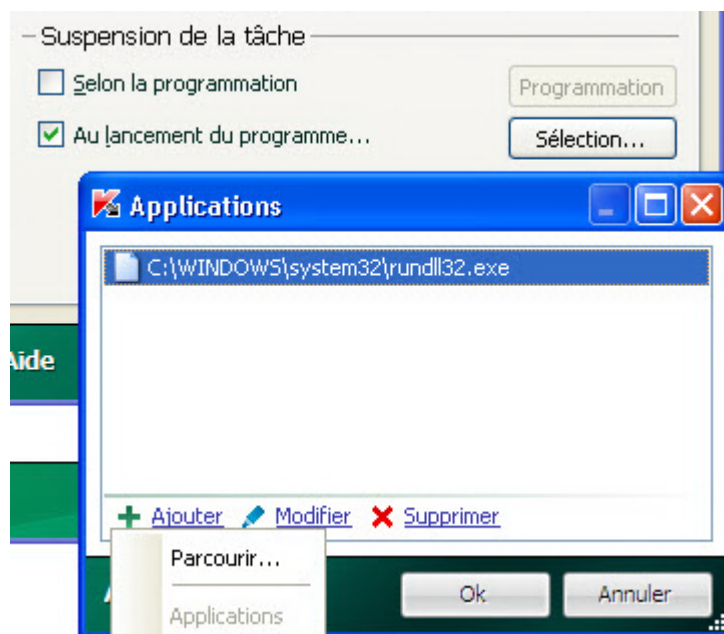


Illustration 8 : Constitution de la liste des applications

La configuration de l'arrêt de l'Antivirus Fichiers en cas de conflits avec des applications déterminées est une mesure extrême ! Si des conflits se sont manifestés pendant l'utilisation du composant, contactez le Service d'assistance technique de Kaspersky Lab (<http://kbsupport.kaspersky.com/fr>). Les experts vous aideront à résoudre les problèmes de compatibilité entre Kaspersky Anti-Virus et les applications de votre ordinateur.

➤ Pour configurer la suspension du composant pendant l'utilisation des applications indiquées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case ☒ **Au lancement de l'application** puis cliquez sur **Sélection**.
5. Dans la fenêtre **Applications** composez la liste des applications pendant l'utilisation desquelles le composant sera suspendu.

RESTAURATION DES PARAMÈTRES DE PROTECTION PAR DÉFAUT

Lorsque vous configurez l'Antivirus Fichiers, vous pouvez décider à n'importe quel moment de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

➡ *Pour restaurer les paramètres de protection par défaut, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Par défaut** dans le groupe **Niveau de protection**.

PROTECTION DU COURRIER

L'*Antivirus Courrier* recherche la présence d'objets dangereux dans le courrier entrant et sortant. Il démarre au lancement du système d'exploitation, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages transmis via les protocoles POP3, SMTP, IMAP, MAPI et NNTP.

L'analyse du courrier se déroule selon un ensemble défini de paramètres désigné sous le concept de niveau de protection. Une fois menace découverte, Antivirus Courrier exécute l'action définie (cf. section "Modification de l'action à réaliser sur les objets identifiés" à la page [54](#)). Les règles d'analyse du courrier sont définies à l'aide de paramètres. Ils peuvent être scindés selon les groupes qui définissent les détails suivants :

- Flux protégé de messages ;
- Utilisation des méthodes d'analyse heuristique ;
- Analyse des fichiers composés ;
- Filtrage des fichiers joints.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Courrier. Dans la majorité des cas, il suffit de sélectionner un autre niveau de protection. Vous pouvez restaurer les paramètres de fonctionnement par défaut de l'Antivirus Courrier. Pour ce faire, sélectionnez un des niveaux de protection.

➡ Afin de modifier les paramètres de fonctionnement de l'Antivirus Courrier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Modifiez les paramètres du composant selon vos besoins.

DANS CETTE SECTION

Algorithme de fonctionnement du composant.....	53
Modification du niveau de protection du courrier.....	53
Modification de l'action à réaliser sur les objets identifiés	54
Constitution de la zone de protection	55
Analyse du courrier dans Microsoft Office Outlook	55
Analyse du courrier dans The Bat!.....	56
Utilisation de l'analyse heuristique	56
Analyse des fichiers composés.....	57
Filtrage des pièces jointes	57
Restauration des paramètres de protection du courrier par défaut	58

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

Kaspersky Anti-Virus comprend un composant qui analyse le courrier à la recherche d'objets dangereux : il s'agit de l'*Antivirus Courrier*. Il est lancé au démarrage du système d'exploitation, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages envoyés et reçus via les protocoles POP3, SMTP, IMAP, MAPI1 et NNTP ainsi que les messages en mode sécurisé (SSL) via les protocoles POP3 et IMAP.

L'icône dans la zone de notification de la barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence  chaque fois qu'un message est analysé.

La protection du courrier est réalisée par défaut selon l'algorithme suivant :

1. Chaque message envoyé ou reçu par l'utilisateur est intercepté par le composant.
2. Le message est décomposé selon ses parties constitutives, à savoir : l'en-tête du message, le corps du message et la pièce jointe.
3. Le corps et la pièce jointe (y compris les objets OLE) sont soumis à la recherche d'éventuels objets dangereux. Les objets malveillants sont identifiés à l'aide de bases utilisées par Kaspersky Anti-Virus et à l'aide d'un Algorithme heuristique. Les bases contiennent la définition de tous les programmes malveillants connus à ce jour et de leur mode d'infection. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les bases.
4. Les comportements suivants sont envisageables à l'issue de l'analyse :
 - Si le corps du message ou la pièce jointe contient un code malveillant, l'Antivirus Courrier bloque le message, crée une copie de sauvegarde et tente de réparer l'objet. Si la réparation réussit, le message reste accessible à l'utilisateur. Si la réparation échoue, l'objet infecté est supprimé du message. Suite au traitement antivirus, un texte spécial est inclus dans l'objet du message. Ce texte indique que le message a été traité par Kaspersky Anti-Virus.
 - Si le corps du message ou la pièce jointe contient un code semblable à un code malveillant, sans garantie, la partie suspecte du message est placée dans un dossier spécial : la quarantaine.
 - Si aucun code malveillant n'a été découvert dans le message, le destinataire pourra y accéder immédiatement.

Un plug-in spécial (cf. section "Analyse du courrier dans Microsoft Office Outlook" à la page [55](#)) qui permet de réaliser une configuration plus fine de l'analyse du courrier a été ajouté à Microsoft Office Outlook.

Si vous utilisez The Bat!, Kaspersky Anti-Virus peut être utilisé conjointement à d'autres logiciels antivirus. Dans ce cas, les règles de traitement du courrier (cf. section "Analyse du courrier dans The Bat!" à la page [56](#)) sont définies directement dans The Bat! et prévalent sur les paramètres de protection du courrier de l'application.

S'agissant des autres clients de messagerie (dont Microsoft Outlook Express, Mozilla Thunderbird, Eudora, Incredimail), l'Antivirus Courrier analyse le courrier entrant et sortant via les protocoles SMTP, POP3, IMAP et NNTP.

N'oubliez pas qu'en cas d'utilisation du client de messagerie Thunderbird, les messages transmis via le protocole IMAP ne sont pas analysés si des filtres pour le transfert des messages depuis le répertoire **Courrier entrant** sont utilisés.

MODIFICATION DU NIVEAU DE PROTECTION DU COURRIER

Le niveau de protection désigne un ensemble prédéfini de paramètres de l'Antivirus Courrier. Les experts de Kaspersky Lab ont configuré trois niveaux de protection. La sélection du niveau de protection est déterminée par l'utilisateur en fonction des conditions de travail et la situation en vigueur. Vous avez le choix parmi les niveaux de protection suivant :

- **Elevé.** Si vous travaillez dans un environnement dangereux, le niveau de protection maximale du courrier sera préférable. Parmi les environnements dangereux, citons la connexion à un service de messagerie en ligne gratuit depuis votre domicile sans protection centralisée du courrier.

- **Recommandé.** Ce niveau assure l'équilibre optimal entre les performances et la sécurité et convient à la majorité des cas. Il est sélectionné par défaut.
- **Bas.** Si vous travaillez dans un environnement bien protégé, le niveau faible sera suffisant. Parmi ce genre d'environnement, citons le réseau d'une entreprise dotée d'un système centralisé de protection du courrier.

Si aucun des niveaux proposés ne répond pas à vos besoins, vous pouvez configurer les paramètres de fonctionnement (cf. section "Protection du courrier" à la page [52](#)) de l'Antivirus Courrier. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut du composant, sélectionnez un des niveaux proposés.

➡ *Afin de modifier le niveau de protection du courrier, exécutez l'opération suivante :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Définissez le niveau de protection requis pour le composant sélectionné.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS IDENTIFIES

L'Antivirus Courrier analyse le message électronique. Si l'analyse antivirus d'un message électronique indique que le message ou l'un de ses objets (corps ou pièce jointe) est infecté ou soupçonné d'être infecté, la suite des opérations du composant dépendra du statut de l'objet et de l'action sélectionnée.

Suite à l'analyse, l'Antivirus Courrier attribue un des états suivants aux objets trouvés :

- Etat de l'un des programmes malveillants (exemple, *virus, cheval de Troie*) ;
- *Probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le message ou la pièce jointe contient une séquence de code d'un virus inconnu ou le code modifié d'un virus connu.

Kaspersky Anti-Virus vous avertira s'il découvre des objets infectés ou potentiellement infectés suite à l'analyse du courrier. Vous devrez réagir à la menace en sélectionnant une action à exécuter sur l'objet. Par défaut, ce comportement de Kaspersky Anti-Virus définit quand l'action à exécuter sur l'objet sélectionné est **Confirmer l'action**. Vous pouvez modifier l'action. Par exemple, si vous êtes convaincu chaque objet découvert doit être soumis à une tentative de réparation et que vous ne souhaitez pas à chaque fois choisir l'option **Réparer** au moment de recevoir la notification sur la découverte d'un objet infecté ou suspect, vous pourrez choisir l'option **Exécuter l'action. Réparer**.

Avant de réparer ou de supprimer un objet, Kaspersky Anti-Virus crée une copie de sauvegarde au cas où la restauration de l'objet serait requise ou si la possibilité de le réparer se présentait.

Si vous travaillez en mode automatique (cf. section "Etape. Sélection du mode de protection" à la page [28](#)), Kaspersky Anti-Virus appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants l'action sera **Réparer. Supprimer si la réparation est impossible et pour les objets suspects : Ignorer**.

➡ *Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Désignez l'action requise pour le composant sélectionné.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone d'analyse désigne les types de message qu'il faut analyser. Kaspersky Anti-Virus analyse par défaut aussi bien les messages entrant que les messages sortant. Si vous avez choisi l'analyse uniquement des messages entrant, il est conseillé au tout début de l'utilisation de Kaspersky Anti-Virus d'analyser le courrier sortant car le risque existe que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. Cela permet d'éviter les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre ordinateur.

La zone de protection reprend également les paramètres d'intégration de l'Antivirus Courrier dans le système ainsi que les protocoles analysés. Par défaut, l'Antivirus Courrier s'intègre aux clients de messagerie Microsoft Office Outlook et The Bat!.

➤ *Pour désactiver la protection du courrier sortant, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Général** dans le groupe **Zone d'analyse**, définissez les paramètres requis.

➤ *Pour sélectionner les paramètres d'intégration de l'Antivirus Courrier au système ainsi que les protocoles à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Intégration au système** sélectionnez les paramètres requis.

ANALYSE DU COURRIER DANS MICROSOFT OFFICE OUTLOOK

Si votre client de messagerie est Microsoft Office Outlook, vous pouvez réaliser une configuration avancée de l'analyse du courrier.

Un module externe spécial est intégré à Microsoft Office Outlook lors de l'installation de Kaspersky Anti-Virus. Il vous permet de passer rapidement à la configuration des paramètres de l'Antivirus Courrier et de définir à quel moment la recherche d'éventuels objets dangereux sera lancée.

Le plug-in prend la forme de l'onglet **Protection du courrier** dans le menu **Services** → **Paramètres**. Sur l'onglet vous pouvez définir le mode du contrôle du courrier.

➤ *Pour définir le mode d'analyse du courrier, procédez comme suit :*

1. Ouvrez la fenêtre principale de Microsoft Office Outlook.
2. Sélectionnez le point **Service** → **Paramètres** dans le menu du programme.
3. Sélectionnez le mode requis d'analyse du courrier sur l'onglet **Protection du courrier**.

ANALYSE DU COURRIER DANS THE BAT!

Les actions à réaliser sur les objets infectés des messages électroniques dans The Bat! sont définies par le programme en lui-même.

Les paramètres de l'Antivirus Courrier qui définissent la nécessité d'analyser le courrier entrant et sortant ainsi que les actions sur les objets dangereux ou les exclusions sont ignorés. Le seul élément pris en compte par The Bat!, c'est l'analyse des archives en pièce jointe.

Les paramètres de protection du courrier sont appliqués à tous les modules antivirus de l'ordinateur compatibles avec The Bat!

Il convient de se rappeler que lors de la réception de messages, ceux-ci sont d'abord analysés par l'Antivirus Courrier puis uniquement après par le module externe pour le client de messagerie The Bat! Kaspersky Anti-Virus vous préviendra sans faute en cas de découverte d'un objet malveillant. Si vous avez sélectionné l'action **Réparer** (**Supprimer**) dans la fenêtre de notification de l'Antivirus Courrier, alors c'est l'Antivirus Courrier qui se chargera des actions de suppression de la menace. Si vous choisissez **Ignorer** dans la fenêtre de notification, alors l'objet sera neutralisé par le module externe de The Bat! Lors de l'envoi de courrier, les messages sont d'abord analysés par le module externe puis par l'Antivirus Courrier.

Vous devez définir :

- Le flux de messagerie qui sera soumis à l'analyse (courrier entrant, sortant).
- Le moment auquel aura lieu l'analyse des objets du message (à l'ouverture du message, avant l'enregistrement sur le disque).
- Les actions exécutées par le client de messagerie en cas de découverte d'objets dangereux dans les messages électroniques. Vous pouvez par exemple choisir :
 - **Tenter de réparer les parties infectées** : si cette option est choisie, l'application tentera de réparer l'objet infecté et si cette réparation est impossible, l'objet restera dans le message.
 - **Supprimer les parties infectées** : si cette option est choisie, l'objet dangereux sera supprimé du message qu'il soit infecté ou potentiellement infecté.

Par défaut, tous les objets infectés des messages sont placés en quarantaine par The Bat! sans réparation.

Les messages électroniques qui contiennent des objets dangereux ne sont pas différenciés dans The Bat! par un titre spécial.

➡ Pour passer à la configuration de la protection du courrier indésirable dans The Bat!, procédez comme suit :

1. Ouvrez la fenêtre principale de The Bat!
2. Sélectionnez l'élément **Configuration** dans le menu **Propriétés** du client de messagerie.
3. Sélectionnez le nœud **Protection contre les virus** dans l'arborescence des paramètres.

UTILISATION DE L'ANALYSE HEURISTIQUE

La méthode heuristique consiste à analyser l'activité de l'objet dans le système. Si cet activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Ainsi, les nouvelles menaces seront identifiées avant que leur activité ne soit remarquée par les spécialistes des virus. L'analyse heuristique est activée par défaut.

Kaspersky Anti-Virus vous signale la découverte d'un objet malveillant dans le message du client de messagerie instantanée. Il convient de réagir à ce message en choisissant une action.

Vous pouvez aussi définir le niveau de détail de l'analyse : **superficielle**, **moyenne** ou **profonde**. Il suffit de déplacer le curseur sur la position souhaitée.

➡ *Pour activer / désactiver l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Méthodes d'analyse**, cochez / décochez la case ☒ **Analyse heuristique** et définissez le niveau de détail de l'analyse en dessous.

ANALYSE DES FICHIERS COMPOSES

La sélection du mode d'analyse des fichiers composés exerce une influence sur les performances de Kaspersky Anti-Virus. Vous pouvez activer ou désactiver l'analyse des archives jointes et limiter la taille maximale des archives à analyser.

➡ *Pour configurer les paramètres d'analyse des fichiers composés, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Général**, sélectionnez le mode d'analyse des fichiers composés.

FILTRAGE DES PIÈCES JOINTES

Vous pouvez configurer les conditions de filtrage des objets joints aux messages. L'utilisation d'un filtre offre une protection supplémentaire car les programmes malveillants se propagent via le courrier électronique sous la forme de pièces jointes. Le changement de nom ou la suppression de la pièce jointe permet de protéger votre ordinateur contre l'exécution automatique d'une pièce jointe à la réception du message.

Si votre ordinateur n'est protégé par aucun moyen du réseau local et si l'accès à Internet s'opère sans serveur proxy ou pare-feu, il est conseillé de ne pas désactiver l'analyse des archives en pièce jointe.

➡ *Pour configurer le filtrage des pièces jointes, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Filtre des pièces jointes**, définissez les conditions de filtrage des objets joints au message. Lorsque les deux derniers modes sont sélectionnés, la liste des types d'objet devient active. Elle vous permet de sélectionner les types requis ou d'ajouter un masque d'un nouveau type.

Si l'ajout du masque du nouveau type est indispensable, cliquez sur le lien **Ajouter** et dans la fenêtre **Masque de nom de fichier** qui s'ouvre, saisissez les données requises.

RESTAURATION DES PARAMETRES DE PROTECTION DU COURRIER PAR DEFAUT

Lorsque vous configurez l'Antivirus Courrier, vous pouvez décider à n'importe quel moment de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

➡ *Pour restaurer les paramètres de protection de courrier par défaut, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Par défaut** dans le groupe **Niveau de protection**.

PROTECTION DU TRAFIC INTERNET

Chaque fois que vous utilisez Internet, vous exposez les données conservées sur votre ordinateur à un risque d'infection par des programmes dangereux. Ils peuvent s'infiltrer dans votre ordinateur tandis que vous téléchargez des programmes gratuits ou que vous consultez des informations sur des sites apparemment inoffensifs (mais soumis à des attaques de pirates avant votre visite). De plus, les vers de réseau peuvent s'introduire sur votre ordinateur avant l'ouverture des pages Web ou le téléchargement d'un fichier, à savoir directement dès l'ouverture de la connexion Internet.

Le composant *Antivirus Internet* a été développé pour protéger votre ordinateur durant l'utilisation d'Internet. Il protège les informations reçues via le protocole HTTP et empêche l'exécution des scripts dangereux.

La protection Internet prévoit le contrôle du trafic http qui transite uniquement via les ports indiqués dans la liste des ports contrôlés. La liste des ports le plus souvent utilisés pour le transfert du courrier et du trafic HTTP est livrée avec le logiciel. Si vous utilisez des ports absents de cette liste, vous devrez les ajouter afin de protéger le trafic qui transite via ces derniers.

Si vous utilisez Internet dans un environnement dépourvu de protection, il est conseillé d'utiliser l'Antivirus Internet. Si votre ordinateur fonctionne dans un réseau protégé par un pare-feu ou des filtres de trafic HTTP, l'Antivirus Internet vous offrira une protection supplémentaire.

L'analyse du trafic se déroule selon un ensemble défini de paramètres désigné sous le concept de niveau de protection. Quand l'Antivirus Internet découvre une menace, il exécute l'action définie.

Le niveau de protection du trafic Internet sur votre ordinateur est défini par un ensemble de paramètres. Ils peuvent être scindés selon les groupes suivants :

- Les paramètres qui définissent la zone protégée ;
- Les paramètres qui définissent la productivité de la protection du trafic (utilisation de l'analyse heuristique, optimisation de l'analyse).

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Internet. Dans la majorité des cas, il suffit de sélectionner un autre niveau de protection.

➡ Afin de modifier les paramètres de fonctionnement de l'Antivirus Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Modifiez les paramètres du composant selon vos besoins.

DANS CETTE SECTION

Algorithme de fonctionnement du composant.....	60
Modification du niveau de protection du trafic HTTP	61
Modification de l'action à réaliser sur les objets identifiés	61
Constitution de la zone de protection	62
Sélection du type d'analyse	62
Module d'analyse des liens.....	63
Utilisation de l'analyse heuristique	64
Optimisation de l'analyse.....	64
Restauration des paramètres de protection Internet par défaut	65

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

L'*Antivirus Internet* protège les informations reçues via le protocole HTTP et empêche l'exécution des scripts dangereux.

Examinons les détails du fonctionnement de ce composant. La protection du trafic HTTP s'opère selon l'algorithme suivant :

1. Chaque page ou fichier qui reçoit une requête de l'utilisateur ou d'un programme quelconque via le protocole HTTP est intercepté et analysé par l'Antivirus Internet pour découvrir la présence de code malveillant. L'identification des objets malveillants est réalisée à l'aide des bases utilisées par Kaspersky Anti-Virus et d'un algorithme heuristique. Les bases contiennent la définition de tous les programmes malveillants connus à ce jour et de leur mode d'infection. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les bases.
2. Les comportements suivants sont possibles en fonction des résultats de l'analyse :
 - Si la page Web ou l'objet que souhaite ouvrir l'utilisateur contient un code malveillant, l'accès est bloqué. Dans ce cas, un message apparaît à l'écran pour avertir l'utilisateur que l'objet ou la page demandée est infecté.
 - Si aucun code malveillant n'a été découvert dans le fichier ou la page Web, l'utilisateur pourra y accéder immédiatement.

L'analyse des scripts est réalisée selon l'algorithme suivant :

1. Chaque script lancé sur une page Web est intercepté par l'Antivirus Internet et soumis à une analyse antivirus.
2. Si le script contient un code malveillant, l'Antivirus Internet le bloque et avertit l'utilisateur à l'aide d'un message contextuel.
3. Si le script ne contient aucun code malicieux, il est exécuté.

Les scripts sont uniquement interceptés dans les pages ouvertes dans Microsoft Internet Explorer

MODIFICATION DU NIVEAU DE PROTECTION DU TRAFIC HTTP

Le niveau de protection désigne un ensemble prédéfini de paramètres de l'Antivirus Internet. Les experts de Kaspersky Lab ont configuré trois niveaux de protection. La sélection du niveau de protection est déterminée par l'utilisateur en fonction des conditions de travail et la situation en vigueur. Vous avez le choix entre un des niveaux de protection suivant :

- **Elevé.** Ce niveau de protection est recommandé dans les milieux agressifs lorsque d'autres moyens de protection du trafic HTTP ne sont pas prévus.
- **Recommandé.** Ce niveau de protection est le niveau optimum pour la majorité des situations.
- **Bas.** Ce niveau est recommandé si votre ordinateur est doté de moyens complémentaires de protection du trafic HTTP.

Si aucun des niveaux proposés ne répond pas à vos besoins, vous pouvez configurer les paramètres de fonctionnement (cf. section "Protection du trafic Internet" à la page [59](#)) de l'Antivirus Internet. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut du composant, sélectionnez un des niveaux proposés.

➡ Afin de modifier le niveau de sécurité défini du trafic Internet, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Définissez le niveau de protection requis pour le composant sélectionné.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS IDENTIFIES

Si l'analyse d'un objet du trafic HTTP détermine la présence d'un code malveillant, la suite des opérations dépendra de l'action que vous aurez spécifiée.

S'agissant des actions sur les scripts dangereux, l'Antivirus Internet bloque toujours leur exécution et affiche à l'écran une infobulle qui informe l'utilisateur sur l'action exécutée. La modification de l'action à réaliser sur un script dangereux n'est pas possible. Seule la désactivation du fonctionnement du module d'analyse des scripts est autorisée (cf. section "Sélection du type d'analyse" à la page [62](#)).

Si vous travaillez en mode automatique (cf. section "Etape. Sélection du mode de protection" à la page [28](#)), Kaspersky Anti-Virus appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux.

➡ Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Désignez l'action requise pour le composant sélectionné.

CONSTITUTION DE LA ZONE DE PROTECTION

La constitution de la zone d'analyse signifie la sélection du type d'analyse (cf. section "Sélection du type d'analyse" à la page 62) des objets par l'Antivirus Internet et la création d'une liste d'URL de confiance dont les données ne seront pas analysées par le composant pour voir si elles contiennent des objets dangereux.

Vous pouvez composer la liste des URL de confiance dont le contenu ne présente absolument aucun danger. L'Antivirus Internet n'analysera pas les informations en provenance de ces adresses. Cela peut être utile lorsque l'antivirus Internet gêne le téléchargement d'un certain fichier qui est à chaque fois bloqué par l'antivirus Internet.

➡ *Pour constituer la liste des URL de confiance, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Optimisation de l'analyse** cochez la case ☒ **Ne pas analyser le trafic HTTP en provenance des URL de confiance** puis cliquez sur **Sélection**.
5. Dans la fenêtre **Liste des URL de confiance** qui s'ouvre, cliquez sur **Ajouter**.
6. Dans la fenêtre **Masque d'adresse (URL)** qui s'ouvre, saisissez l'adresse de confiance (ou son masque).

SELECTION DU TYPE D'ANALYSE

La tâche de composition de la zone d'analyse (cf. page 62) propose également, outre la création d'une liste d'URL de confiance, la possibilité de choisir le type d'analyse du trafic par Antivirus Internet. Les analyses proposées sont l'analyse des scripts et l'analyse du trafic HTML.

Par défaut, l'Antivirus Internet analyse le trafic HTTP et les scripts simultanément.

L'analyse du trafic HTTP désigne non seulement la recherche de virus mais également la vérification des liens afin de voir s'ils appartiennent à la liste des URL suspectes et/ou de phishing.

L'analyse des liens pour vérifier s'ils appartiennent à la liste des adresses de phishing permet d'éviter les attaques de phishing qui, en règle générale, se présentent sous la forme de messages électroniques prétendument envoyés par une institution financière et qui contiennent des liens vers le site de ces institutions. Le texte du message amène le destinataire à cliquer sur le lien et à saisir des données confidentielles (numéro de carte de crédit, code d'accès aux services de banque en ligne) sur la page qui s'affiche.

Puisque le lien vers un site de phishing peut être envoyé non seulement par courrier électronique, mais également par d'autres moyens tels que les messages ICQ, le composant Antivirus Internet suit les tentatives d'ouverture du site de phishing au niveau de l'analyse du trafic HTTP et les bloque.

La vérification des liens pour voir s'ils appartiennent à la liste des URL suspectes permet de repérer les sites qui figurent sur la liste noire. La liste est composée par les experts de Kaspersky Lab et est livrée avec l'application.

➡ *Pour qu'Antivirus Internet analyse les scripts, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre **Antivirus Internet**, qui s'ouvre, dans le groupe **Avancé**, assurez-vous que la case ☒ **Bloquer les scripts dangereux dans Microsoft Internet Explorer** est cochée. L'Antivirus Internet analysera tous les scripts traités par Microsoft Internet Explorer ainsi que n'importe quel script WSH (JavaScript, Visual Basic Script, etc.) lancé tandis que l'utilisateur travaille sur l'ordinateur, notamment sur Internet.

De plus, vous pouvez utiliser le module d'analyse des liens (cf. page 63) en cochant la case ☒ **Signaler les liens suspects ou d'hameçonnage dans Microsoft Internet Explorer et Mozilla Firefox**. L'Antivirus Internet mettra en évidence dans les navigateurs (Microsoft Internet Explorer et Mozilla Firefox) les liens suspects ou d'hameçonnage dans les URL.

➡ *Pour vérifier si un lien appartient à la liste des URL suspectes et/ou de phishing, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Méthodes d'analyse**, assurez-vous que la case ☒ **Analyser les liens selon la base des URL suspectes** et / ou la case ☒ **Analyser les liens selon la base des URL de phishing** sont cochées.

MODULE D'ANALYSE DES LIENS

Kaspersky Anti-Virus propose un module d'analyse des liens qui est administré par l'Antivirus Internet. Le module analyse tous les liens sur une page afin de voir s'il s'agit de liens suspects ou de phishing. Vous pouvez composer la liste des adresses de confiance des sites dont le contenu ne doit pas être analysé ainsi que la liste des sites dont le contenu doit absolument être analysé. Le module est intégré aux navigateurs Microsoft Internet Explorer et Mozilla Firefox sous la forme d'un plug-in.

➡ *Pour activer le module d'analyse des liens, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Avancé** cochez la case ☒ **Signaler les liens suspects ou d'hameçonnage dans Microsoft Internet Explorer et Mozilla Firefox**.

➡ *Pour constituer la liste des URL de confiance, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Avancé** cliquez sur le bouton **Configuration**.
5. Dans la fenêtre **Module d'analyse des liens** qui s'ouvre, sélectionnez l'option  **Pour toutes les pages Internet** puis cliquez sur le bouton **Exclusions**.
6. Dans la fenêtre **Liste des URL de confiance** qui s'ouvre, cliquez sur **Ajouter**.
7. Dans la fenêtre **Masque d'adresse (URL)** qui s'ouvre, saisissez l'adresse de confiance (ou son masque).

➤ Pour composer la liste des URL des sites dont le contenu doit absolument être analysé, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Avancé** cliquez sur le bouton **Configuration**.
5. Dans la fenêtre **Module d'analyse des liens** qui s'ouvre, sélectionnez l'option  **Pour les pages Internet indiqués** puis cliquez sur le bouton **Sélection**.
6. Dans la fenêtre **Liste des URL analysées** qui s'ouvre, cliquez sur **Ajouter**.
7. Dans la fenêtre **Masque d'adresse (URL)** qui s'ouvre, saisissez l'adresse (ou son masque).

UTILISATION DE L'ANALYSE HEURISTIQUE

La méthode heuristique consiste à analyser l'activité de l'objet dans le système. Si cet activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Ainsi, les nouvelles menaces seront identifiées avant que leur activité ne soit remarquée par les spécialistes des virus. L'analyse heuristique est activée par défaut.

Kaspersky Anti-Virus vous signale la découverte d'un objet malveillant dans le message du client de messagerie instantanée. Il convient de réagir à ce message en choisissant une action.

Vous pouvez qui plus est définir le niveau de détail de l'analyse : **superficiel**, **moyen** ou **profond**. Il suffit de déplacer le curseur sur la position souhaitée.

➤ Pour activer / désactiver l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Méthodes d'analyse**, cochez / décochez la case  **Analyse heuristique** et définissez le niveau de détail de l'analyse en dessous.

OPTIMISATION DE L'ANALYSE

Afin d'accroître le taux de détection des codes malveillants, l'Antivirus Internet utilise la technologie de mise en cache de fragments des objets envoyés via Internet. Dans cette méthode, l'analyse est réalisée uniquement une fois que l'objet entier a été reçu. Ensuite, l'objet est soumis à une recherche de virus et il est transmis à l'utilisateur ou bloqué en fonction des résultats de cette analyse.

Sachez toutefois que la mise en cache augmente la durée de traitement de l'objet et du transfert à l'utilisateur. Elle peut également provoquer des problèmes au niveau de la copie et du traitement de gros objets en raison de l'écoulement du délai de connexion du client HTTP.

Pour résoudre ce problème, nous vous proposons de limiter dans le temps la mise en cache des fragments des objets. Une fois le délai écoulé, chaque partie du fichier reçue sera transmise à l'utilisateur sans vérification et l'objet sera analysé complètement une fois qu'il sera copié. Ainsi, la durée du transfert de l'objet à l'utilisateur est réduite et les problèmes liés à la déconnexion sont réglés sans pour autant réduire le niveau de la protection pendant l'utilisation d'Internet.

Par défaut, la limitation dans le temps de la mise en cache des fragments est de 1 seconde. L'augmentation de cette valeur ou la levée de la restriction de la durée de la mise en cache augmente le niveau de l'analyse antivirus mais entraîne un certain ralentissement au niveau de l'accès à l'objet.

➡ *Pour établir une restriction dans le temps pour la mise en cache des fragments ou pour lever cette restriction, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Optimisation de l'analyse**, cochez / décochez la case ☒ **Limitier la durée de mise en cache des fragments** et définissez le temps (en secondes) dans le champ de droite.

RESTAURATION DES PARAMETRES DE PROTECTION INTERNET PAR DEFAUT

Lorsque vous configurez l'Antivirus Internet, vous pouvez décider à n'importe quel moment de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

➡ *Pour restaurer les paramètres de l'Antivirus Internet par défaut, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Par défaut** dans le groupe **Niveau de protection**.

PROTECTION DU TRAFIC DES MESSAGERIES INSTANTANÉES

Les applications très populaires ces derniers temps pour l'échange de messages instantanés (par la suite, les *clients de messagerie instantanée*) facilitent la communication via Internet mais constituent également une menace pour la sécurité de l'ordinateur. Les clients de messagerie instantanée peuvent envoyer des messages contenant des liens vers des sites suspects ou vers des sites utilisés par les individus mal intentionnés pour les attaques d'hameçonnage. Les programmes malveillants utilisent les clients de messagerie instantanée pour diffuser des messages non sollicités et des liens vers des programmes (ou les programmes eux-mêmes) développés pour dérober le compte de l'utilisateur.

Le composant *Antivirus IM ("Chat")* a été mis au point pour garantir votre protection durant l'utilisation de clients de messagerie instantanée. Il protège les informations envoyées vers votre ordinateur via les protocoles des clients de messagerie instantanée.

Ce logiciel garantit une utilisation sans danger des systèmes de messagerie instantanée tels qu'ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, etc.

Les applications Yahoo! Messenger et Google Talk fonctionnent via le protocole SSL. Pour que l'Antivirus IM analyse le trafic de ces applications, il faut utiliser l'analyse des connexions sécurisées (cf. page [110](#)). Pour ce faire, cochez la case ☒ **Analyse des connexions sécurisées** dans la section **Réseau**.

L'analyse du trafic est réalisée selon un ensemble défini de paramètres. Dès que l'Antivirus IM détecte une menace dans un message, il remplace le contenu du message par un avertissement pour l'utilisateur.

Le niveau de protection du trafic des messageries instantanées sur votre ordinateur est défini par un ensemble de paramètres. Ils peuvent être scindés selon les groupes suivants :

- Paramètres définissant la zone d'analyse ;
- Paramètres définissant les méthodes d'analyse.

➡ Afin de modifier les paramètres de fonctionnement de l'Antivirus IM, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Pour le composant sélectionné, modifiez comme il se doit les paramètres.

DANS CETTE SECTION

Algorithme de fonctionnement du composant.....	67
Constitution de la zone de protection	67
Sélection de la méthode d'analyse.....	67
Utilisation de l'analyse heuristique	68

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

Kaspersky Anti-Virus propose un composant qui analyse les messages transmis via les clients de messagerie instantanée afin de voir s'il contiennent des objets dangereux. Il s'agit d'*Antivirus IM ("Chat")*. Il est lancé en même temps que le système d'exploitation, demeure en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages entrant ou sortant.

Par défaut, la protection du trafic des clients de messagerie instantanée s'opère selon l'algorithme suivant.

1. Chaque message envoyé ou reçu par l'utilisateur est intercepté par le composant.
2. Antivirus IM analyse le message afin de voir s'il contient des objets dangereux ou des liens repris dans les bases des URL suspectes ou de phishing. Lorsqu'une menace est détectée, le texte du message est remplacé par un avertissement à l'attention de l'utilisateur.
3. Si aucune menace pour la sécurité n'est détectée, le message est accessible à l'utilisateur.

Les fichiers transmis via les clients de messagerie instantanée sont analysés par le composant Antivirus Fichiers (cf. section "Protection du système de fichiers de l'ordinateur" à la page 42) au moment de la tentative de sauvegarde.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone d'analyse désigne les types de message qu'il faut analyser :

-  **Analyser le courrier entrant et sortant.** L'Antivirus IM ("Chat") analyse par défaut les messages entrant et sortant.
-  **Analyser uniquement le courrier entrant.** Si vous êtes convaincu que les messages que vous envoyez ne peuvent contenir d'objets dangereux, sélectionnez ce paramètre. L'Antivirus IM analysera uniquement les messages entrant.

Kaspersky Anti-Virus analyse par défaut aussi bien les messages entrant que les messages sortant des clients de messagerie instantanée.

Si vous êtes convaincu que les messages que vous envoyez ne peuvent contenir aucun objet dangereux, vous pouvez vous passer de l'analyse du trafic sortant.

➡ *Pour désactiver l'analyse des messages sortant, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Pour le composant sélectionné, choisissez l'option  **Analyser uniquement le courrier entrant** dans le groupe **Zone d'analyse**.

SELECTION DE LA METHODE D'ANALYSE

La méthode d'analyse désigne l'analyse des liens, inclus dans les messages envoyés par messagerie instantanée, pour savoir s'ils appartiennent à la liste des adresses suspectes et / ou à la liste des adresses de phishing :

-  **Analyser les liens selon la base des URL suspectes.** L'Antivirus IM analysera les liens dans les messages afin de voir s'ils appartiennent à la liste noire.

- ☒ **Analyser les liens selon la base des URL de phishing.** Les bases de Kaspersky Anti-Virus contiennent les sites connus à l'heure actuelle qui sont utilisés lors des attaques de phishing. Les experts de Kaspersky Lab y ajoutent les adresses fournies par l'organisation internationale de lutte contre le phishing (The Anti-Phishing Working Group). Cette liste est enrichie lors de la mise à jour des bases de Kaspersky Anti-Virus.

➤ *Pour analyser les liens des messages selon la base des adresses suspectes, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cochez la case ☒ **Analyser les liens selon la base des URL suspectes** dans le groupe **Méthodes d'analyse**.

➤ *Pour analyser les liens des messages selon la base des adresses de phishing, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cochez la case ☒ **Analyser les liens selon la base des URL de phishing** dans le groupe **Méthodes d'analyse**.

UTILISATION DE L'ANALYSE HEURISTIQUE

La méthode heuristique consiste à analyser l'activité de l'objet dans le système. C'est ainsi que tout script contenu dans un message d'un client de messagerie instantanée est exécuté dans un milieu sûr. Si l'activité du script est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. L'analyse heuristique est activée par défaut.

Kaspersky Anti-Virus vous signale la découverte d'un objet malveillant dans le message du client de messagerie instantanée.

Vous pouvez aussi sélectionner le niveau de détail de l'analyse : **superficielle**, **moyenne** ou **profonde**. Il suffit de déplacer le curseur sur la position souhaitée.

➤ *Pour activer / désactiver l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cochez ou décochez la case ☒ **Analyse heuristique** dans le groupe **Méthodes d'analyse** puis établissez le niveau de détail de l'analyse.

DEFENSE PROACTIVE

Kaspersky Anti-Virus offre une protection non seulement contre les menaces connues mais également contre les nouvelles menaces qui ne figurent pas dans les bases de Kaspersky Anti-Virus. Cette possibilité est garantie par un composant développé spécialement – la *Défense Proactive*.

Les technologies préventives sur lesquelles repose la défense proactive évitent ces pertes de temps et permettent de neutraliser la nouvelle menace avant qu'elle n'ait pu nuire à votre ordinateur. A la différence des technologies réactives qui réalisent l'analyse selon les enregistrements des bases de Kaspersky Anti-Virus, les technologies préventives identifient les nouvelles menaces en suivant les séquences d'actions exécutées par une application quelconque. Si l'analyse de la séquence d'actions de l'application éveille des soupçons, Kaspersky Anti-Virus bloque l'activité de cette application.

➡ Afin de modifier les paramètres de fonctionnement de la *Défense Proactive*, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.
3. Pour le composant sélectionné, introduisez les modifications requises dans les paramètres.

DANS CETTE SECTION

Utilisation de la liste des activités dangereuses	69
Modification d'une règle de contrôle de l'activité dangereuse	70
Constitution d'un groupe d'applications de confiance	71
Contrôle des comptes utilisateur système	71

UTILISATION DE LA LISTE DES ACTIVITES DANGEREUSES

N'oubliez pas que la configuration du contrôle de l'activité dans Kaspersky Anti-Virus installée sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64 est différente de la configuration pour Kaspersky Anti-Virus installées sous d'autres systèmes d'exploitation.

Particularités de la configuration du contrôle de l'activité des applications sous Microsoft Windows XP

Kaspersky Anti-Virus surveille l'activité des applications sur votre ordinateur. La Défense Proactive réagit à une séquence définie d'actions de l'application quelconque. Ainsi, si un programme se copie dans une ressource de réseau, dans le répertoire de démarrage, dans la base de registres et qu'il diffuse ces copies, on peut affirmer sans crainte qu'il s'agit d'un ver. Parmi les séquences d'actions dangereuses, citons également :

- actions typiques des chevaux de Troie ;
- tentative d'interception des saisies au clavier ;
- installation cachée de pilotes ;
- tentative de modification du noyau du système d'exploitation ;
- tentative de création d'objets cachés et de processus avec un identifiant (PID) négatif ;
- tentative de modification du fichier HOSTS ;

- tentative d'intrusion dans un autre processus ;
- apparition d'un processus cherchant à réorienter les données entrantes/sortantes ;
- tentative d'envoi des demandes DNS.

La liste des activités dangereuses est remplie automatiquement lors de la mise à jour de Kaspersky Anti-Virus et il est impossible de la modifier. Vous pouvez néanmoins refuser de contrôler une activité dangereuse.

➡ *Pour refuser de contrôler une activité dangereuse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.
3. Pour le composant sélectionné, le bouton **Configuration**.
4. Dans la fenêtre **Défense Proactive** qui s'ouvre, décochez la case ☒ située en regard du nom de l'activité dont vous refusez le contrôle.

Particularités de la configuration du contrôle de l'activité des applications sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64

Si l'ordinateur tourne sous un des systèmes d'exploitation cités ci-dessus, alors certains événements ne seront pas contrôlés. Ceci s'explique par les particularités de ces systèmes d'exploitation. Ainsi, les types suivants d'événements ne seront pas contrôlés : *intrusion dans un autre processus, envoi des données par les applications de confiance, activité suspecte dans le système, accès au stockage protégé.*

MODIFICATION D'UNE REGLE DE CONTROLE DE L'ACTIVITE DANGEREUSE

La liste des activités dangereuses est remplie automatiquement lors de la mise à jour de Kaspersky Anti-Virus et il est impossible de la modifier. Vous pouvez :

- refuser de contrôler une activité quelconque (cf. page [69](#)) ;
- modifier la règle qui définit le fonctionnement de la défense proactive lors de la découverte d'activités dangereuses.
- composer une liste d'exclusions (cf. page [107](#)), reprenant les applications que vous n'estimez pas dangereuses.

➡ *Afin de modifier une règle, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.
3. Pour le composant sélectionné, le bouton **Configuration**.
4. Dans la fenêtre **Défense Proactive** qui s'ouvre, dans le groupe **Evénements** sélectionnez l'événement nécessaire, pour lequel la règle sera modifiée.
5. Pour l'événement sélectionné, configurez les paramètres nécessaires de la règle à l'aide des liens dans le bloc de description de la règle :
 - cliquez sur le lien indiquant l'action établie et dans la fenêtre **Sélection des actions** ouverte, sélectionnez l'action nécessaire parmi les actions proposées ;

- cliquez sur le lien indiquant la période (n'est pas définie pour tous les types d'activité) et dans la fenêtre **Découverte des processus cachés** ouverte, indiquez l'intervalle selon lequel la recherche de découverte des processus cachés s'exécutera ;
- cliquez sur le lien Act. / Désact., pour indiquer la nécessité de créer un rapport sur l'opération exécutée.

CONSTITUTION D'UN GROUPE D'APPLICATIONS DE CONFIANCE

Vous pouvez exploiter la possibilité de définir le cercle de programmes de confiance dont l'activité ne sera pas analysée par la Défense Proactive. Les applications de confiance peuvent être les applications possédant une signature numérique (Editeurs connus) ou les applications présentes dans la base de Kaspersky Security Network.

➤ *Pour que la Défense proactive considère comme programme de confiance tout programme doté d'une signature numérique ou repris dans la base de Kaspersky Security Network et ne vous communique aucune information relative à l'activité, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cochez les cases ☒ **Avec une signature numérique (Editeurs connus)** et / ou ☒ **Présentes dans la base de Kaspersky Security Network** dans le groupe **Applications de confiance**.

CONTROLE DES COMPTES UTILISATEUR SYSTEME

Les comptes utilisateur réglementent l'accès au système et définissent l'utilisateur et son environnement de travail, ce qui permet d'éviter d'endommager le système d'exploitation ou les données des autres utilisateurs. Les processus système sont les processus qui ont été lancés par le compte système.

➤ *Pour que Kaspersky Anti-Virus surveille l'activité des processus système, ceci excluant les processus utilisateurs, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cochez la case ☒ **Contrôler les comptes Systèmes** dans le groupe **Avancé**.

ANALYSE DE L'ORDINATEUR

La recherche de virus et de vulnérabilités sur l'ordinateur est une des principales tâches qui garantira la protection de l'ordinateur. L'analyse met en évidence la diffusion d'un code malveillant qui, pour une raison quelconque, n'avait pas été découvert par la protection contre les programmes malveillants. La recherche de vulnérabilités détermine si les applications présentent des vulnérabilités qui pourraient être exploitées par les individus mal intentionnés pour diffuser des objets malveillants et accéder aux données personnelles.

Les experts de Kaspersky Lab ont élaboré des tâches d'analyse (cf. page [72](#)), dont l'analyse des disques amovibles (cf. page [78](#)), et la tâche de recherche de vulnérabilités dans le système et les applications (cf. page [82](#)).

➡ Pour modifier les paramètres d'une tâche d'analyse quelconque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des objets**, **Recherche de Vulnérabilités**).
3. Introduisez les modifications requises dans les paramètres de la tâche sélectionnée.

DANS CETTE SECTION

Recherche de virus	72
Recherche de vulnérabilités	82

RECHERCHE DE VIRUS

Les experts de Kaspersky Lab ont identifiés les tâches suivantes pour la recherche de virus sur votre ordinateur :

- **Analyse des objets.** Les objets sélectionnés par l'utilisateur sont analysés. L'analyse peut porter sur n'importe quel objet du système de fichiers de l'ordinateur. Dans le cadre de cette tâche, vous pouvez configurer l'analyse des disques amovibles.
- **Analyse Complète.** Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.
- **Analyse Rapide.** L'analyse porte sur les objets chargés au démarrage du système d'exploitation.

Les tâches d'analyse rapide et complète sont des tâches spécifiques. Il est déconseillé de modifier la liste des objets à analyser pour ces tâches.

Chaque tâche d'analyse est exécutée dans une zone définie et peut être lancée selon un horaire défini. L'ensemble des paramètres des tâches d'analyse définissent le niveau de protection. Il existe trois niveaux par défaut.

Après le lancement de la tâche d'analyse, la progression de cette dernière est présentée dans la rubrique **Analyse** de la fenêtre principale de Kaspersky Anti-Virus dans le champ **Dernière exécution** sous le nom de la tâche exécutée. Quand l'application découvre une menace, elle exécute l'action définie.

Les informations sur les résultats de la recherche de menaces sont consignées dans le rapport de Kaspersky Anti-Virus.

De plus, vous pouvez sélectionner l'objet à analyser via les outils standard du système d'exploitation Microsoft Windows (par exemple : via l'**Assistant** ou sur le **Bureau**, etc.). Pour ce faire, placez la souris sur l'objet, ouvrez le menu contextuel de Microsoft Windows d'un clic droit et sélectionnez **Rechercher d'éventuels virus**.

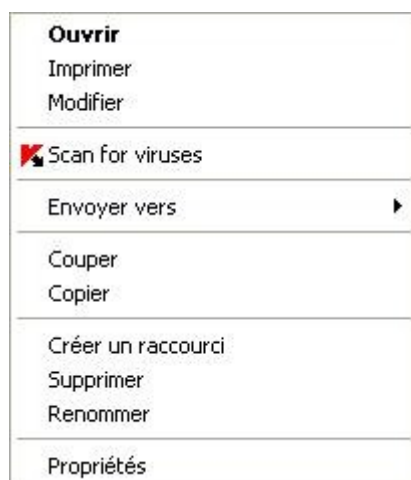


Illustration 9: Menu contextuel de Microsoft Windows

Vous pouvez également accéder au rapport sur l'analyse où vous pourrez voir des informations complètes sur les événements survenus durant l'exécution des tâches.

VOIR ÉGALEMENT

Lancement de l'analyse.....	74
Création de raccourcis pour le lancement d'une tâche.....	75
Composition de la liste des objets à analyser.....	75
Modification du niveau de protection.....	76
Modification de l'action à exécuter après la découverte d'une menace.....	77
Modification du type d'objets à analyser.....	77
Optimisation de l'analyse.....	78
Analyse des disques amovibles.....	78
Analyse des fichiers composés.....	79
Technologie d'analyse.....	80
Modification de la méthode d'analyse	80
Mode de lancement : programmation.....	81
Mode de lancement : configuration du compte utilisateur.....	81
Particularité du lancement programmé des tâches de l'analyse	82
Restauration des paramètres d'analyse par défaut.....	82

LANCEMENT DE L'ANALYSE

L'analyse peut être lancée des manières suivantes :

- depuis le menu contextuel (cf. section "Menu contextuel" à la page [38](#)) de Kaspersky Anti-Virus ;
- depuis la fenêtre principale (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page [39](#)) de Kaspersky Anti-Virus ;
- via un raccourci créé (cf. page [75](#)) au préalable.

Les informations relatives à l'exécution de la tâche sont affichées dans la fenêtre principale de Kaspersky Anti-Virus.

De plus, vous pouvez sélectionner l'objet à analyser via les outils standard du système d'exploitation Microsoft Windows (exemple : via l'**Assistant** ou sur le **Bureau**, etc.).

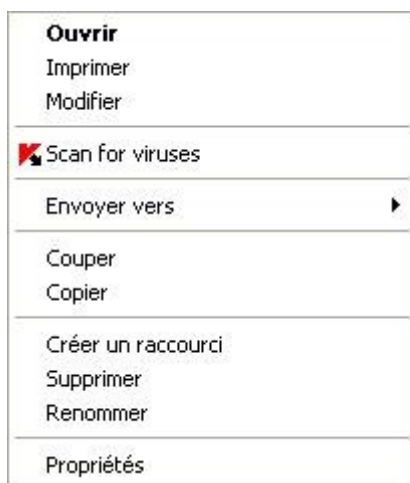


Illustration 10: Menu contextuel de Microsoft Windows

➤ Pour lancer une tâche à l'aide d'un raccourci, procédez comme suit :

1. Ouvrez le répertoire dans lequel vous avez créé le raccourci.
2. Double-cliquez sur le raccourci pour lancer la tâche. La progression de la tâche est illustrée dans la fenêtre principale de Kaspersky Anti-Virus dans la rubrique **Analyse**.

➤ Pour lancer la recherche d'éventuels virus depuis le menu contextuel de l'application, procédez comme suit :

1. Cliquez sur le bouton droit de la souris sur l'icône de l'application dans la zone de notification de la barre des tâches.
2. Dans le menu qui s'ouvre, sélectionnez le point **Rechercher d'éventuels virus**.
3. Dans la fenêtre principale de Kaspersky Anti-Virus qui s'ouvre, dans la rubrique **Analyse**, cliquez sur le bouton portant le nom de la tâche qui vous intéresse.

Pour lancer l'analyse complète de l'ordinateur, choisissez l'option **Analyse complète de l'ordinateur** dans le menu contextuel. L'analyse complète de l'ordinateur sera lancée. La progression de la tâche est illustrée dans la fenêtre principale de Kaspersky Anti-Virus dans la rubrique **Analyse**.

➤ *Pour lancer la recherche d'éventuels virus depuis la fenêtre principale de l'application :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Cliquez sur le bouton portant le nom de la tâche qui vous intéresse.

➤ *Pour lancer la recherche d'éventuels virus dans un objet sélectionné depuis le menu contextuel de Microsoft Windows, procédez comme suit :*

1. Cliquez avec le bouton droit de la souris sur le nom de l'objet sélectionné.
2. Dans le menu contextuel qui s'ouvre, sélectionnez le point **Rechercher d'éventuels virus**. La progression et le résultat d'exécution de la tâche sont illustrés dans la fenêtre ouverte.

CREATION DE RACCOURCIS POUR LE LANCEMENT D'UNE TACHE

Il est possible de créer des raccourcis pour accélérer le lancement des analyses complètes et rapides. Il est ainsi possible de lancer la tâche d'analyse requise sans devoir ouvrir la fenêtre principale de l'application ou le menu contextuel.

➤ *Pour créer un raccourci pour le lancement de l'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Dans la partie droite de la fenêtre, dans le groupe **Lancement rapide des tâches**, cliquez sur le lien **Créer un raccourci** situé à côté du nom de la tâche envisagée (**Analyse Rapide** ou **Analyse Complète**).
4. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès pour l'enregistrement du fichier ainsi que le nom de celui-ci. Par défaut, le raccourci prend le nom de la tâche et est créé dans le répertoire *Poste de travail* de l'utilisateur actuel de l'ordinateur.

COMPOSITION DE LA LISTE DES OBJETS A ANALYSER

Une liste d'objets à analyser est associée par défaut à chaque tâche de recherche d'éventuels virus. Ces objets peuvent être des objets du système de fichiers de l'ordinateur (par exemple, les disques logiques, les **bases de messagerie**) ainsi que des objets d'autres types (par exemple, des disques de réseau). Vous pouvez introduire des modifications dans cette liste.

L'objet ajouté apparaît désormais dans la liste. Si au moment d'ajouter l'objet, vous avez coché la case ☒ **Sous-répertoires compris**, l'analyse se fera à tous les niveaux.

Pour supprimer un objet de la liste, sélectionnez-le et cliquez sur le lien **Supprimer**.

Les objets ajoutés à la liste par défaut ne peuvent être modifiés ou supprimés.

Outre la suppression des objets, il est possible également de les exclure temporairement de l'analyse. Pour ce faire, sélectionnez l'objet dans la liste et désélectionnez la case située à gauche de son nom.

Si la couverture d'analyse est vide ou si aucun des objets qu'elle contient n'a été coché, il ne sera pas possible de lancer la tâche d'analyse !

➤ *Pour constituer la liste des objets de l'analyse des objets, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Cliquez sur le lien **Ajouter**.
4. Dans la fenêtre **Sélection de l'objet à analyser** qui s'ouvre, sélectionnez l'objet et cliquez sur le bouton **Ajouter**. Une fois que vous aurez ajoutés les objets requis, cliquez sur le bouton **OK**. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

➤ *Pour composer la liste des objets pour les analyses complète ou rapide, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Analyse Complète (Analyse Rapide)**.
3. Pour la tâche sélectionnée, dans le groupe **Objets à analyser**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **<Nom de l'analyse>: liste des objets** qui s'ouvre, constituez la liste à l'aide des liens **Ajouter**, **Modifier**, **Supprimer**. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

MODIFICATION DU NIVEAU DE PROTECTION

Le niveau de protection désigne un ensemble prédéfini de paramètres d'analyse. Les experts de Kaspersky Lab ont configuré trois niveaux de protection : Vous choisissez le niveau en fonction de vos préférences. Vous avez le choix parmi les niveaux de protection suivants :

- **Elevé.** Choisissez ce niveau si vous estimez que le risque d'infection de votre ordinateur est élevé.
- **Recommandé.** Ce niveau convient à la majorité des cas et son utilisation est conseillée par les experts de Kaspersky Lab.
- **Bas.** Si vous utilisez des applications gourmandes en mémoire vive, sélectionnez le niveau faible car la sélection de fichiers à analyser à ce niveau est moindre.

Si aucun des niveaux proposés ne répond à vos besoins, vous pouvez configurer vous-même les paramètres de fonctionnement. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut de l'analyse, sélectionnez un des niveaux proposés.

➤ *Afin de modifier le niveau de protection, exécutez l'opération suivante :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée, dans le groupe **Niveau de protection**, définissez le niveau requis.

MODIFICATION DE L'ACTION A EXECUTER APRES LA DECOUVERTE D'UNE MENACE

Quand Kaspersky Anti-Virus découvre une menace, il lui attribue un des états suivants :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*) ;
- *Probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le fichier contient une séquence de code d'un virus inconnu ou le code modifié d'un virus connu.

Kaspersky Anti-Virus vous avertira s'il découvre des objets infectés ou potentiellement infectés suite à l'analyse. Il faut réagir à la menace découverte à l'aide d'une action sur l'objet. En cas de sélection de l'option **Confirmer l'action** pour les actions à réaliser sur l'objet identifié, le comportement de Kaspersky Anti-Virus sera le comportement par défaut. Vous pouvez modifier l'action. Par exemple, si vous êtes convaincu chaque objet découvert doit être soumis à une tentative de réparation et que vous ne souhaitez pas à chaque fois choisir l'option **Réparer** au moment de recevoir la notification sur la découverte d'un objet infecté ou suspect, choisissez l'option **Exécuter l'action. Réparer**.

Avant de réparer ou de supprimer un objet, Kaspersky Anti-Virus crée une copie de sauvegarde au cas où la restauration de l'objet serait requise ou si la possibilité de le réparer se présentait.

Si vous travaillez en mode automatique (cf. section "Etape. Sélection du mode de protection" à la page 28), Kaspersky Anti-Virus appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants l'action sera **Réparer. Supprimer si la réparation est impossible et pour les objets suspects : Ignorer**.

➡ Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée, dans le groupe **Action**, désignez l'action requise.

MODIFICATION DU TYPE D'OBJETS A ANALYSER

La définition du type d'objet à analyser est la fonction qui vous permet d'indiquer le format et la taille des fichiers qui seront analysés lors de l'exécution de la tâche d'analyse sélectionnée.

Il convient de ne pas oublier les caractéristiques suivantes des types de fichiers au moment de les sélectionner :

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple *txt*) et son activation ultérieure est relativement faible. Il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, *exe*, *dll*, *doc*). Le risque d'infection par un code malveillant et d'activation est assez élevé pour ces fichiers.
- Il ne faut pas oublier qu'un individu mal intentionné peut envoyer un virus dans un fichier portant l'extension *txt* alors qu'il s'agit en fait d'un fichier exécutable renommé en fichier *txt*. Si vous sélectionnez l'option  **Fichiers analysés selon l'extension**, ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option  **Fichiers analysés selon le format**, la protection des fichiers et de la mémoire ignorera l'extension, analysera l'en-tête du fichier et découvrira qu'il s'agit d'un fichier *exe*. Le fichier sera alors soumis à une analyse antivirus minutieuse.

➤ Afin de modifier la priorité de la règle, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Types de fichiers** sélectionnez le paramètre requis.

OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée de l'analyse et accélérer le fonctionnement de Kaspersky Anti-Virus. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

Il est également possible de limiter la durée de l'analyse. Une fois la durée écoulée, l'analyse des fichiers sera suspendue.

➤ Afin d'analyser uniquement les nouveaux fichiers et les fichiers modifiés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Optimisation de l'analyse** cochez la case ☒ **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

➤ Pour définir une restriction temporaire sur la durée de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sur l'onglet **Zone d'action**, groupe **Optimisation de l'analyse**, cochez la case ☒ **Arrêter l'analyse si elle dure plus de**, et définissez la durée d'analyse dans le champ à côté.

ANALYSE DES DISQUES AMOVIBLES

Ces derniers temps, les objets malveillants qui exploitent les vulnérabilités du système d'exploitation pour se diffuser via les réseaux locaux et les disques amovibles se sont fort répandus.

Vous pouvez analyser les disques amovibles au moment où ils sont connectés à l'ordinateur. Pour ce faire, il faut sélectionner une des actions qu'exécutera Kaspersky Anti-Virus.

- **Ne pas analyser.** L'analyse automatique des disques amovibles connectés à l'ordinateur ne sera pas réalisée.
- **Confirmer auprès de l'utilisateur.** Par défaut, Kaspersky Anti-Virus demande à l'utilisateur de confirmer l'action à exécuter lorsque le disque amovible est connecté à l'ordinateur.

- **Analyse Complète.** Une fois que le disque amovible est connecté à l'ordinateur, les fichiers qu'il contient (selon les paramètres de la tâche Analyse Complète) sont soumis à une analyse complète.
- **Analyse Rapide.** Seuls les objets de démarrage (selon les paramètres de la tâche Analyse Rapide) sont analysés lorsque le disque amovible est connecté à l'ordinateur.

➡ *Afin de pouvoir analyser les disques amovibles lorsqu'ils sont connectés à l'ordinateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Dans le groupe **Analyse des disques amovibles à la connexion**, sélectionnez l'action et, le cas échéant, définissez la taille maximale du disque à analyser dans le champ inférieur.

ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés (archives, bases de données, etc.) est une pratique très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour ce faire, cliquez sur le lien situé en regard du nom de l'objet. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si vous sélectionnez le mode d'analyse uniquement des nouveaux fichiers et des fichiers modifiés (cf. page 78), il sera impossible de sélectionner un type de fichier composé.

Vous pouvez également définir la taille maximale du fichier composé à analyser. Les fichiers composés dont la taille dépasse la valeur limite ne seront pas analysés.

L'analyse des fichiers de grande taille au moment de l'extraction des archives aura lieu même si la case ☒ **Ne pas décompacter les fichiers composés de grande taille** est cochée.

➡ *Pour modifier la liste des fichiers composés à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le bloc **Analyse des fichiers composés** sélectionnez les types de fichiers composés à analyser.

➡ *Pour définir la taille maximale des fichiers composés qui seront analysés, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Zone d'action**.
5. Dans la fenêtre **Fichiers composés** qui s'ouvre, cochez la case ☒ **Ne pas décompacter les objets composés de grande taille** et définissez la taille maximale des objets à analyser dans le champ en dessous.

TECHNOLOGIE D'ANALYSE

Vous pouvez indiquer également la technologie qui sera utilisée lors de l'analyse. Vous avez le choix entre les technologies suivantes :

- **iChecker.** Cette technologie permet d'accélérer l'analyse en excluant certains objets. L'exclusion d'un objet de l'analyse est réalisée à l'aide d'un algorithme spécial qui tient compte de la date d'édition des signatures des menaces, de la date de l'analyse antérieure et de la modification des paramètres d'analyse.

Admettons que vous avez une archive qui a été analysée par Kaspersky Anti-Virus et auquel il a attribué l'état *non infecté*. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases de l'application, l'archive sera analysée à nouveau.

La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et de plus, elle n'est applicable qu'aux objets dont la structure est connue de l'application (exemple : fichiers exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift.** Cette technologie est un développement de la technologie iChecker pour les ordinateurs dotés d'un système de fichiers NTFS. Il existe certaines restrictions à la technologie iSwift : elle s'applique à l'emplacement particulier d'un fichier dans le système de fichiers et elle ne s'applique qu'aux objets des systèmes de fichiers NTFS.

➡ Afin de modifier la technologie d'analyse des objets, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Technologies d'analyse**, définissez les paramètres requis.

MODIFICATION DE LA METHODE D'ANALYSE

Vous pouvez configurer certains paramètres d'analyse qui ont une influence sur la minutie de celle-ci. Le mode de recherche des menaces à l'aide des signatures des bases de l'application est toujours activé par défaut. De plus, il est possible d'agir sur diverses méthodes et technologies d'analyse (cf. page [80](#)).

Le mode d'analyse à l'aide des signatures où Kaspersky Anti-Virus compare l'objet trouvé aux enregistrements de la base est toujours utilisé. Vous pouvez également choisir d'utiliser l'analyse heuristique. Cette méthode repose sur l'analyse de l'activité de l'objet dans le système. Si l'activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect.

Il est également possible de choisir le niveau de détails de l'analyse heuristique : superficiel, moyen ou profond. Il suffit de déplacer le curseur sur la position souhaitée.

Outre ces méthodes d'analyse, vous pouvez également utiliser la recherche d'outils de dissimulation d'activité. Un outil de dissimulation d'activité est un utilitaire qui permet de dissimuler la présence de programmes malveillants dans le système d'exploitation. Ces utilitaires s'introduisent dans le système en masquant leur présence et celle des processus, des répertoires et des clés de registre de n'importe quel programme malveillant décrit dans la configuration de l'outil de dissimulation d'activité. Lorsque la recherche est activée, vous pouvez définir le niveau de détail d'identification des outils de dissimulation d'activité (Analyse en profondeur). Dans ce cas, une recherche minutieuse de ces programmes sera lancée via l'analyse d'une grande quantité d'objets de divers types.

➤ *Pour utiliser les méthodes d'analyse requises, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Méthodes d'analyse**, définissez les paramètres requis.

MODE DE LANCEMENT : PROGRAMMATION

Il est possible de programmer l'exécution automatique de l'analyse.

L'élément primordial à définir est l'intervalle selon lequel la tâche doit être exécutée. Pour ce faire, il faut définir les paramètres de la programmation pour l'option sélectionnée.

Si l'exécution est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique dès que cela est possible.

➤ *Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation** choisissez **Manuel** si vous souhaitez lancer la tâche d'analyse à l'heure qui vous convient. Pour lancer la tâche à intervalle régulier, sélectionnez l'option **Programmation** et définissez les paramètres d'exécution.

➤ *Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, groupe **Programmation**, cochez la case ☒ **Lancer les tâches non exécutées**.

MODE DE LANCEMENT : CONFIGURATION DU COMPTE UTILISATEUR

Vous pouvez définir le compte utilisateur sous les privilèges duquel la recherche de virus sera réalisée.

➤ *Pour définir le compte utilisé, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).

3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, onglet **Mode d'exécution**, groupe **Utilisateur**, cochez la case ☒ **Lancer la tâche avec les privilèges d'un autre utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

PARTICULARITE DU LANCEMENT PROGRAMME DES TACHES DE L'ANALYSE

Toutes les tâches d'analyse peuvent être lancées manuellement ou automatiquement selon un horaire défini.

Pour les tâches, lancées selon la programmation, vous pouvez utiliser la possibilité complémentaire : *suspendre l'analyse selon la programmation si l'écran de veille est actif ou l'ordinateur est débloqué*. Cette possibilité permet de reporter le lancement de la tâche jusqu'à ce que l'utilisateur ne termine pas son travail sur l'ordinateur. Ainsi, la tâche d'analyse ne va pas occuper les ressources de l'ordinateur pendant son fonctionnement.

➡ Pour lancer l'analyse une fois que l'utilisateur terminera son travail, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation**, cochez la case ☒ **Suspendre l'analyse selon la programmation si l'écran de veille est actif et l'ordinateur est débloqué**.

RESTAURATION DES PARAMETRES D'ANALYSE PAR DEFAUT

Une fois que vous aurez configuré les paramètres d'exécution de la tâche, sachez que vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

➡ Pour restaurer les paramètres de protection des fichiers par défaut, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète, Analyse Rapide, Analyse des objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Par défaut**.

RECHERCHE DE VULNERABILITES

La tâche de recherche de vulnérabilités pose un diagnostic sur la sécurité du système et recherche les éventuelles vulnérabilités qui sont généralement exploitées par les individus mal intentionnés pour nuire.

Dans le cadre de cette étude, le système est analysé et l'application recherche les anomalies ou les corruptions dans les paramètres du système d'exploitation et du navigateur. Le diagnostic de la sécurité s'opère dans de nombreuses directions : par exemple, la recherche d'outils de dissimulation d'activité (programme pour le contrôle dissimulé d'un système compromis), recherche de services ou de paramètres vulnérables, collecte d'informations sur les processus, les pilotes, etc.

Le diagnostic des vulnérabilités peut prendre un certain temps. Une fois que le diagnostic est terminé, les informations recueillies sont analysées. L'analyse vise à évaluer les problèmes identifiés dans la sécurité du point de vue du danger qu'ils représentent pour le système.

Tous les problèmes identifiés au moment de l'analyse du système sont regroupés du point de vue du danger qu'il présente pour le système. Pour chaque groupe de problèmes, les experts de Kaspersky Lab proposent un ensemble d'actions dont l'exécution permettra de supprimer les vulnérabilités et les points problématiques du système. Trois groupes de problèmes et les actions correspondantes ont été identifiés :

- *Les actions vivement recommandées* permettent de supprimer les problèmes qui constituent une menace sérieuse pour la sécurité. Il est conseillé d'exécuter toutes les actions de ce groupe.
- *Les actions recommandées* visent à supprimer les problèmes qui peuvent présenter un danger potentiel. L'exécution des actions de ce groupe est également recommandée.
- *Les actions complémentaires* sont prévues pour supprimer les corruptions du système qui ne présentent actuellement aucun danger mais qui à l'avenir pourraient menacer la sécurité de l'ordinateur.

Les liens directs vers les correctifs critiques (mise à jour des applications) sont les résultats de la recherche des vulnérabilités potentielles dans le système d'exploitation et les applications installées.

Une fois la tâche de recherche de vulnérabilités lancées (cf. page [83](#)), sa progression s'affiche dans la fenêtre principale de l'application et dans la fenêtre **Recherche de Vulnérabilités** dans le champ **Fin**. Les vulnérabilités identifiées dans le système et dans les applications à la suite de l'analyse figurent dans cette même fenêtre sous les onglets **Vulnérabilités du système** et **Applications vulnérables**.

Les informations sur les résultats de la recherche de menaces sont consignées dans le rapport de Kaspersky Anti-Virus.

A l'instar de ce qui se fait pour les tâches d'analyse, il est possible, dans la section **Recherche de Vulnérabilités** de la fenêtre de configuration de l'application, de définir un horaire d'exécution (cf. page [85](#)) et de composer une liste d'objets à analyser (cf. page [84](#)) pour la recherche de vulnérabilités. Par défaut, les applications installées sont choisies en guise d'objets à analyser.

VOIR EGALEMENT

Lancement de la recherche de vulnérabilités	83
Création de raccourcis pour le lancement d'une tâche.....	84
Composition de la liste des objets à analyser.....	84
Mode de lancement : programmation.....	85
Mode de lancement : configuration du compte utilisateur.....	85

LANCEMENT DE LA RECHERCHE DE VULNERABILITES

La recherche de vulnérabilités peut être lancée d'une des manières suivantes :

- depuis la fenêtre principale (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page [39](#)) de Kaspersky Anti-Virus ;
- via un raccourci créé (cf. page [84](#)) au préalable.

Les informations relatives à l'exécution de la tâche sont affichées dans la fenêtre principale de Kaspersky Anti-Virus ainsi que dans la fenêtre **Recherche de Vulnérabilités**.

➤ *Pour lancer une tâche à l'aide d'un raccourci, procédez comme suit :*

1. Ouvrez le répertoire dans lequel vous avez créé le raccourci.
2. Double-cliquez sur le raccourci pour lancer la tâche. La progression de la tâche est illustrée dans la fenêtre principale de l'application.

➤ *Pour lancer la tâche de recherche de vulnérabilités depuis la fenêtre de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Cliquez sur le bouton **Ouvrir la fenêtre de recherche de vulnérabilités**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Lancer la recherche de vulnérabilités**. La progression de la tâche sera présentée dans le champ **Fin**. Pour arrêter l'exécution de la tâche, cliquez à nouveau sur le bouton.

CREATION DE RACCOURCIS POUR LE LANCEMENT D'UNE TACHE

Pour accélérer le lancement de la recherche de vulnérabilités, l'application offre la possibilité de créer un raccourci. Il est ainsi possible de lancer la tâche sans devoir ouvrir la fenêtre principale de l'application.

➤ *Pour créer un raccourci pour le lancement de la recherche de vulnérabilités, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Dans la partie droite de la fenêtre, dans le groupe **Lancement rapide des tâches**, cliquez sur le bouton **Créer un raccourci** à côté du nom de la tâche (**Recherche de Vulnérabilités**).
4. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès pour l'enregistrement du fichier ainsi que le nom de celui-ci. Par défaut, le raccourci prend le nom de la tâche et est créé dans le répertoire *Poste de travail* de l'utilisateur actuel de l'ordinateur.

COMPOSITION DE LA LISTE DES OBJETS A ANALYSER

Par défaut, la recherche de vulnérabilités possède sa propre liste d'objets à analyser. Ces objets sont le système d'exploitation et les applications installées. Il est possible également de désigner des objets complémentaires tels que les objets du système de fichiers de l'ordinateur (par exemple, les disques logiques ou les **Bases de messagerie**) ou des objets d'autres types (par exemple, les disques de réseau).

L'objet ajouté apparaît désormais dans la liste. Si au moment d'ajouter l'objet, vous avez coché la case ☒ **Sous-répertoires compris**, l'analyse se fera à tous les niveaux. Les objets ajoutés manuellement seront également soumis à l'analyse.

Pour supprimer un objet de la liste, sélectionnez-le et cliquez sur le lien **Supprimer**.

Les objets ajoutés à la liste par défaut ne peuvent être modifiés ou supprimés.

Outre la suppression des objets, il est possible également de les exclure temporairement de l'analyse. Pour ce faire, sélectionnez l'objet dans la liste et désélectionnez la case située à gauche de son nom.

Si la couverture d'analyse est vide ou si aucun des objets qu'elle contient n'a été coché, il ne sera pas possible de lancer la tâche d'analyse !

➤ Pour constituer la liste des objets de la recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Recherche de Vulnérabilités** dans la rubrique **Analyse**.
3. Pour la tâche sélectionnée, dans le groupe **Objets à analyser**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Recherche des vulnérabilités: liste des objets** qui s'ouvre, composez la liste à l'aide des liens **Ajouter**, **Modifier**, **Supprimer**. Pour exclure temporairement un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

MODE DE LANCEMENT : PROGRAMMATION

Il est possible de programmer le lancement automatique de la recherche de vulnérabilités.

L'élément principal à déterminer est l'intervalle selon lequel la tâche doit être exécutée.

Si l'exécution est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique dès que cela est possible.

➤ Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Recherche de Vulnérabilités** dans la rubrique **Analyse**.
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation** choisissez **Manuel** si vous souhaitez lancer la tâche d'analyse à l'heure qui vous convient. Pour lancer la tâche à intervalle régulier, sélectionnez l'option **Programmation** et définissez les paramètres d'exécution.

➤ Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Recherche de Vulnérabilités** dans la rubrique **Analyse**.
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, groupe **Programmation**, cochez la case ☒ **Lancer les tâches non exécutées**.

MODE DE LANCEMENT : CONFIGURATION DU COMPTE UTILISATEUR

Vous pouvez définir le compte utilisateur sous les privilèges duquel la recherche de vulnérabilité sera réalisée.

➡ *Pour définir le compte utilisé, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Recherche de Vulnérabilités** dans la rubrique **Analyse**.
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, onglet **Mode d'exécution**, groupe **Utilisateur**, cochez la case ☒ **Lancer la tâche avec les privilèges d'un autre utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

MISE A JOUR

L'actualité de la protection est le garant de la sécurité de votre ordinateur. Chaque jour, de nouveaux virus, chevaux de Troie et autres programmes malveillant apparaissent. Il est donc primordial de s'assurer que vos données sont bien protégées. Les informations relatives aux menaces et aux moyens de les neutraliser sont reprises dans les bases de Kaspersky Anti-Virus et c'est la raison pour laquelle la mise à jour des bases de l'application constitue un élément fondamental pour maintenir la protection d'actualité.

Lors de la mise à jour de l'application, les objets suivants sont téléchargés et installés sur votre ordinateur :

- Bases de Kaspersky Anti-Virus.

La protection des données est garantie par l'utilisation de bases de données qui contiennent les descriptions des signatures des menaces et des attaques de réseau ainsi que les méthodes de lutte contre celles-ci. Elles sont utilisées par les composants de la protection pour rechercher les objets dangereux sur votre ordinateur et les neutraliser. Ces bases sont enrichies régulièrement des définitions des nouvelles menaces et des moyens de lutter contre celles-ci. Pour cette raison, il est vivement recommandé de les actualiser régulièrement.

En plus des bases de Kaspersky Anti-Virus, la mise à jour concerne également les pilotes de réseau qui assurent l'interception du trafic de réseau par les composants de la protection.

- Modules logiciels.

En plus des bases de Kaspersky Anti-Virus, vous pouvez actualiser les modules logiciels. Ces paquets de mise à jour suppriment des vulnérabilités de Kaspersky Anti-Virus, ajoutent de nouvelles fonctions ou améliorent les fonctions existantes.

Les serveurs spéciaux de mise à jour de Kaspersky Lab sont les principales sources pour obtenir les mises à jour de Kaspersky Anti-Virus.

Pour réussir à télécharger les mises à jour depuis les serveurs, il faut que votre ordinateur soit connecté à Internet. Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si les paramètres du serveur proxy ne sont pas définis automatiquement, configurez les paramètres de connexion à ce dernier.

Au cours du processus, les modules logiciels et les bases installés sur votre ordinateur sont comparés à ceux du serveur. Si les bases et les composants installés sur votre ordinateur sont toujours d'actualité, le message correspondant apparaîtra à l'écran. Si les bases et les modules diffèrent, la partie manquante de la mise à jour sera installée. La copie des bases et des modules complets n'a pas lieu, ce qui permet d'augmenter sensiblement la vitesse de la mise à jour et de réduire le volume du trafic.

Si les bases sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Avant de lancer la mise à jour des bases, Kaspersky Anti-Virus réalise une copie des bases installées au cas où vous souhaiteriez à nouveau les utiliser pour une raison quelconque.

La possibilité d'annuler une mise à jour est indispensable, par exemple si les bases que vous avez téléchargées sont corrompues. Vous pouvez ainsi revenir à la version précédente et tenter de les actualiser à nouveau ultérieurement.

Parallèlement à la mise à jour de Kaspersky Anti-Virus, vous pouvez copier les mises à jour obtenues dans une source locale. Ce service permet d'actualiser les bases antivirus et les modules logiciels sur les ordinateurs du réseau en réduisant le trafic Internet.

Vous pouvez également configurer le mode de lancement automatique de la mise à jour.

La section **Mise à jour** de la fenêtre principale de l'application reprend les informations relatives à l'état actuel des bases de Kaspersky Anti-Virus :

- date et heure de diffusion ;
- Quantité et état des enregistrements dans les bases ;
- État des bases (à jour, dépassées ou corrompues).

Vous pouvez passer au rapport sur les mises à jour qui reprend les informations complètes relatives aux événements survenus lors de l'exécution de la tâche de mises à jour (lien **Rapport** dans la partie supérieure de la fenêtre). Vous pouvez également prendre connaissance de l'activité virale sur le site www.kaspersky.com/fr (lien **Examen de l'activité des virus**).

DANS CETTE SECTION

Lancement de la mise à jour.....	88
Annulation de la dernière mise à jour.....	89
Sélection de la source de mises à jour.....	89
Utilisation du serveur proxy	90
Paramètres régionaux.....	90
Actions exécutées après la mise à jour.....	91
Mise à jour depuis un répertoire local	91
Modification du mode de lancement de la tâche de mise à jour.....	92
Lancement de la mise à jour avec les privilèges d'un autre utilisateur	92

LANCEMENT DE LA MISE A JOUR

Vous pouvez lancer la mise à jour de Kaspersky Anti-Virus à n'importe quel moment. Celle-ci sera réalisée au départ de la source de la mise à jour (cf. section "Sélection de la source de mises à jour" à la page [89](#)) que vous aurez choisie..

La mise à jour de Kaspersky Anti-Virus peut être lancée de deux façons :

- depuis le menu contextuel (cf. section "Menu contextuel" à la page [38](#)) ;
- depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page [39](#)).

Les informations relatives au processus sont affichées dans la rubrique **Mise à jour** de la fenêtre principale de l'application.

► *Pour lancer la mise à jour de Kaspersky Anti-Virus depuis le menu contextuel, procédez comme suit :*

1. Cliquez sur le bouton droit de la souris sur l'icône de l'application dans la zone de notification de la barre des tâches.
2. Dans le menu qui s'ouvre, sélectionnez le point **Mise à jour**.

► *Pour lancer la mise à jour de Kaspersky Anti-Virus depuis la fenêtre principale du logiciel, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur **Lancer la Mise à jour**. La progression de la tâche est illustrée dans la fenêtre principale de l'application.

ANNULATION DE LA DERNIERE MISE A JOUR

Chaque fois que vous lancez la mise à jour du logiciel, Kaspersky Anti-Virus crée une copie de sauvegarde de la version actuelle des bases et des modules de l'application utilisés avant de les actualiser. Cela vous donne la possibilité d'utiliser à nouveau les bases antérieures après une mise à jour ratée.

La possibilité de revenir à l'état antérieur de la mise à jour est utile, par exemple, si une partie de la base est corrompue. Les bases locales peuvent être corrompues par l'utilisateur ou par un programme malveillant, ce qui est possible uniquement lorsque l'autodéfense (cf. section "Autodéfense de Kaspersky Anti-Virus" à la page [102](#)) de Kaspersky Anti-Virus est désactivée. Vous pouvez ainsi revenir aux bases antérieures et tenter de les actualiser à nouveau ultérieurement.

► *Pour revenir à l'utilisation de la version précédente des bases, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le bouton **Restaurer les mises à jours précédentes**.

SELECTION DE LA SOURCE DE MISES A JOUR

La *source des mises à jour* est une ressource qui contient les mises à jour des bases et des modules de Kaspersky Anti-Virus. Il peut s'agir d'un serveur HTTP ou FTP, voire d'un répertoire local ou de réseau.

Les serveurs de mise à jour de Kaspersky Lab constituent la source principale de mises à jour. Il s'agit de sites Internet spéciaux prévus pour la diffusion des bases et des modules logiciels pour tous les produits de Kaspersky Lab.

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Lab (ex : pas de connexion à Internet), vous pouvez contacter nos bureaux au +7 (495) 797 87 00 ou au +7 (495) 645-79-39 pour obtenir l'adresse d'un partenaire de Kaspersky Lab qui pourra vous donner la mise à jour sur disquette ou sur CD-ROM dans un fichier zip.

Les mises à jour obtenues sur un disque amovible peuvent être par la suite placées sur un site FTP ou HTTP ou dans un répertoire local ou de réseau.

Lors de la commande des mises à jour sur disque amovible, précisez si vous souhaitez recevoir la mise à jour des modules logiciels.

Par défaut, la liste des sources de mises à jour contient uniquement les serveurs de mise à jour de Kaspersky Lab.

Si en guise de source de mises à jour vous avez sélectionné une ressource située hors de l'intranet, vous devrez être connecté à Internet pour télécharger la mise à jour.

Si plusieurs ressources ont été sélectionnées en guise de sources de mise à jour, Kaspersky Anti-Virus les consultera dans l'ordre de la liste et réalisera la mise à jour au départ de la première source disponible.

➤ *Pour sélectionner la source de la mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Source** cliquez sur le bouton **Ajouter**.
5. Dans la fenêtre **Sélection de la source des mises à jour** qui s'ouvre, sélectionnez le site FTP ou HTTP ou saisissez son adresse IP, son nom symbolique ou son adresse URL.

UTILISATION DU SERVEUR PROXY

Si vous vous connectez à Internet via un serveur proxy, il faudra le configurer.

➤ *Pour configurer les paramètres du serveur proxy, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Source** cliquez sur le bouton **Serveur proxy**.
5. Dans la fenêtre **Paramètres du serveur proxy** qui s'ouvre, configurez les paramètres du serveur proxy.

PARAMETRES REGIONAUX

Si vous utilisez les serveurs de Kaspersky Lab en guise de serveur de mise à jour, vous pouvez sélectionner le serveur en fonction de la situation géographique qui vous convient le mieux. Les serveurs de Kaspersky Lab sont répartis entre plusieurs pays. En choisissant le serveur situé le plus proche de vous géographiquement, vous pouvez augmenter la vitesse de la mise à jour et du téléchargement de celle-ci.

➤ *Pour sélectionner le serveur le plus proche, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre sous l'onglet **Source**, dans le groupe **Paramètres régionaux**, cochez la case  **Choisir dans la liste** et, dans la liste déroulante, sélectionnez le pays le plus proche de votre situation géographique actuelle.

Si vous choisissez l'option  **Déterminer automatiquement**, la mise à jour utilisera les informations sur la région définie dans la base de registre du système d'exploitation.

ACTIONS EXECUTEES APRES LA MISE A JOUR

Kaspersky Anti-Virus permet également de définir les actions qui seront exécutées automatiquement après la mise à jour. Les actions suivantes peuvent être sélectionnées :

- **Analyser les fichiers en quarantaine.** La quarantaine contient des objets dont l'analyse n'a pas pu définir avec certitude le type de programme malicieux qui les a infectés. Il se peut que les bases puissent identifier catégoriquement la menace après la mise à jour et la supprimer. C'est pour cette raison que le logiciel analyse les objets en quarantaine après chaque mise à jour. Nous vous conseillons d'examiner fréquemment les objets en quarantaine. Leur statut peut changer après l'analyse. Certains objets pourront être restaurés dans leur emplacement d'origine et être à nouveau utilisés.
- **Copier la mise à jour des bases dans le dossier.** Si les ordinateurs font partie d'un réseau local, il n'est pas nécessaire de télécharger et d'installer les mises à jour sur chacun des postes séparés car cela entraînerait une augmentation du trafic. Vous pouvez utiliser le mécanisme de copie des mises à jour qui permet de réduire le trafic en procédant une seule fois au téléchargement de la mise à jour.

➡ *Pour analyser les fichiers en quarantaine après la mise à jour, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Avancé**, cochez la case ☒ **Analyser les fichiers en quarantaine après mise à jour**.

MISE A JOUR DEPUIS UN REPERTOIRE LOCAL

La procédure de récupération des mises à jour depuis un répertoire local est organisée de la manière suivante :

1. Un des ordinateurs du réseau récupère les mises à jour pour Kaspersky Anti-Virus sur les serveurs de Kaspersky Lab ou sur tout autre serveur en ligne proposant les mises à jour les plus récentes. Les mises à jour ainsi obtenues sont placées dans un dossier partagé.
2. Les autres ordinateurs du réseau accèdent à ce dossier partagé afin d'obtenir les mises à jour de Kaspersky Anti-Virus.

➡ *Pour activer le mode de copie des mises à jour, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Avancé**, cochez la case ☒ **Copier la mise à jour des bases dans le dossier** et dans le champ en dessous, saisissez le chemin d'accès au dossier partagé où seront stockées les mises à jour récupérées. Vous pouvez aussi saisir le chemin dans la fenêtre qui s'ouvre dès que vous aurez cliqué sur **Parcourir**.

➡ *Afin que la mise à jour soit réalisée depuis le répertoire partagé sélectionné, réalisez les opérations suivantes sur tous les ordinateurs du réseau :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Source** cliquez sur le bouton **Ajouter**.

5. Dans la fenêtre **Sélection de la source des mises à jour** qui s'ouvre, sélectionnez le répertoire ou saisissez son chemin d'accès complet dans le champ **Source**.
6. Dans l'onglet **Source** désélectionnez la case ☒ **Serveurs de mises à jour de Kaspersky Lab**.

MODIFICATION DU MODE DE LANCEMENT DE LA TACHE DE MISE A JOUR

Le mode de lancement de la tâche de mise à jour de Kaspersky Anti-Virus est sélectionné lors du fonctionnement de l'Assistant de configuration de l'application (cf. section "Étape 3. Configuration de la mise à jour de l'application" à la page 28). Si le mode d'exécution de la mise à jour sélectionné ne vous convient pas, vous pouvez le changer.

L'exécution de la tâche de mise à jour peut se dérouler selon l'un des modes suivants :

-  **Automatique**. Kaspersky Anti-Virus vérifie, selon un intervalle déterminé, si un paquet de mise à jour se trouve dans la source. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Si le logiciel découvre des nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur.
-  **Selon la programmation** (l'intervalle peut changer en fonction des paramètres de programmation). La mise à jour sera lancée automatiquement selon l'horaire défini.
-  **Manuel**. Vous lancez vous-même la procédure de mise à jour de Kaspersky Anti-Virus.

➡ *Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, onglet **Mode d'exécution**, groupe **Programmation**, sélectionnez le mode d'exécution de la mise à jour. Si vous avez choisi l'option  **Selon la programmation**, définissez l'horaire.

Si pour une raison quelconque le lancement de la mise à jour a été ignoré (par exemple, votre ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique des tâches ignorées dès que cela sera possible. Pour ce faire, cochez la case ☒ **Lancer les tâches non exécutées** dans la partie inférieure de la fenêtre. Cette case est accessible pour toutes les options de programmation à l'exception de **Heures**, **Minutes** et **Après le lancement de l'application**.

LANCEMENT DE LA MISE A JOUR AVEC LES PRIVILEGES D'UN AUTRE UTILISATEUR

La mise à jour est lancée par défaut sous le compte que vous avez utilisé pour ouvrir votre session. Il arrive parfois que la mise à jour de Kaspersky Anti-Virus se déroule depuis une source à laquelle vous n'avez pas accès (par exemple, le répertoire de réseau contenant des mises à jour) ou pour laquelle vous ne jouissez pas des privilèges d'utilisateur autorisé du serveur proxy. Vous pouvez lancer la mise à jour de Kaspersky Anti-Virus au nom d'un utilisateur qui possède de tels privilèges.

➡ Pour lancer la mise à jour avec les privilèges d'un autre utilisateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, onglet **Mode d'exécution**, groupe **Utilisateur**, cochez la case ☒ **Lancer la tâche avec les privilèges d'un autre utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

CONFIGURATION DES PARAMETRES DE L'APPLICATION

La fenêtre de configuration des paramètres de l'application vous permet d'accéder rapidement aux paramètres principaux de Kaspersky Anti-Virus.

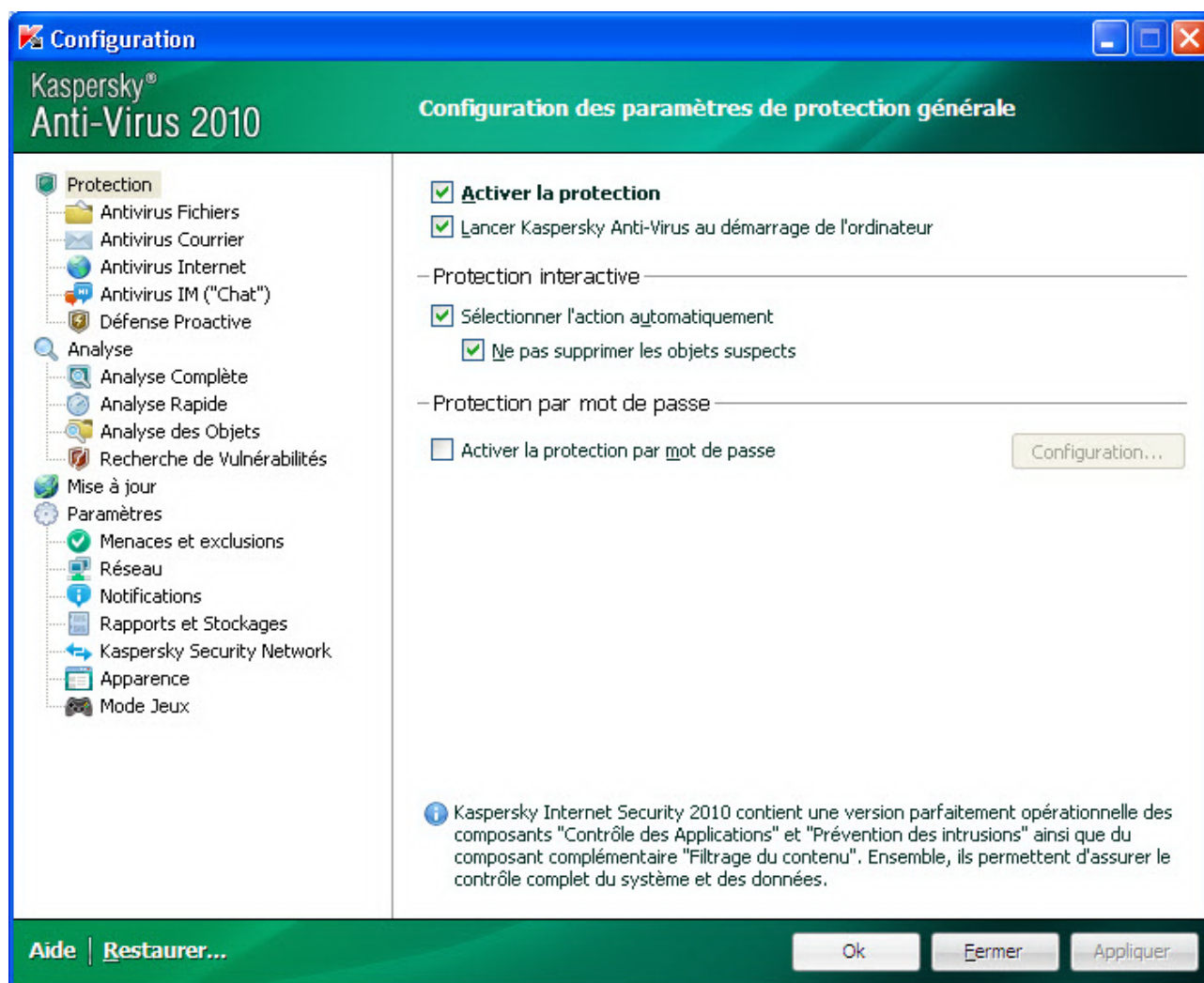


Illustration 11 : Fenêtre de configuration des paramètres de l'application

La fenêtre de configuration contient deux parties :

- la partie gauche permet d'accéder au composant de Kaspersky Anti-Virus, aux tâches de recherche de virus, à la mise à jour, etc. ;
- la partie droite reprend une énumération des paramètres du composant, de la tâche, etc. sélectionnés dans la partie gauche.

Vous pouvez ouvrir la fenêtre d'une des manières suivantes :

- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Anti-Virus" à la page 39). Pour ce faire, cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

- Depuis le menu contextuel (cf. section "Menu contextuel" à la page [38](#)). Pour ce faire, sélectionnez l'élément **Configuration** dans le menu contextuel de l'application.



Illustration 12: Menu contextuel

DANS CETTE SECTION

Protection	95
Antivirus Fichiers	97
Antivirus Courrier	98
Antivirus Internet	99
Antivirus IM ("Chat")	100
Défense Proactive	100
Analyse	101
Mise à jour	102
Paramètres	102

PROTECTION

La fenêtre **Protection** vous permet d'utiliser les fonctions avancées suivantes de Kaspersky Anti-Virus :

- Activation / désactivation de la protection de Kaspersky Anti-Virus (cf. page [95](#)).
- Lancement de Kaspersky Anti-Virus au démarrage du système d'exploitation (cf. page [96](#)).
- Utilisation du mode de protection interactif (cf. page [96](#)).
- Restriction de l'accès à Kaspersky Anti-Virus (cf. page [97](#)).

ACTIVATION / DESACTIVATION DE LA PROTECTION DE L'ORDINATEUR

Kaspersky Anti-Virus est lancé par défaut au démarrage du système d'exploitation et protège votre ordinateur pendant la session. Tous les composants de la protection sont activés.

Vous pouvez désactiver totalement ou partiellement la protection offerte par Kaspersky Anti-Virus.

Les experts de Kaspersky Lab vous recommandent vivement de **ne pas désactiver la protection** car cela pourrait entraîner l'infection de l'ordinateur et la perte de données.

Cette action entraînera l'arrêt de tous ses composants. Les éléments suivants en témoignent :

- l'icône de l'application dans la zone de notification de la barre des tâches est en grise ;
- la couleur rouge de l'indicateur de sécurité.

Notez que dans ce cas, la protection est envisagée dans le contexte des composants du logiciel. La désactivation du fonctionnement des composants de la protection n'a pas d'influence sur la recherche de virus et la mise à jour de Kaspersky Anti-Virus.

➡ *Pour désactiver complètement la protection, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Protection**.
3. Désélectionnez la case ☒ **Activer la protection**.

LANCEMENT DE KASPERSKY ANTI-VIRUS AU DEMARRAGE DU SYSTEME D'EXPLOITATION

Si pour une raison quelconque vous devez arrêter d'utiliser Kaspersky Anti-Virus, sélectionnez le point **Terminer** dans le menu contextuel (cf. section "Menu contextuel" à la page 38) de Kaspersky Anti-Virus. Le programme sera déchargé de la mémoire vive de l'ordinateur. Cela signifie que votre ordinateur ne sera plus protégé pendant cette période.

Vous pouvez réactiver la protection de l'ordinateur en chargeant Kaspersky Anti-Virus via le menu **Démarrer** → **Programmes** → **Kaspersky Anti-Virus 2010** → **Kaspersky Anti-Virus 2010**.

Il est possible également de lancer la protection automatiquement après le redémarrage du système d'exploitation.

➡ *Pour activer ce mode, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Protection**.
3. Cochez la case ☒ **Lancer Kaspersky Anti-Virus au démarrage de l'ordinateur**.

UTILISATION DU MODE DE PROTECTION INTERACTIF

Kaspersky Anti-Virus interagit avec l'utilisateur selon deux modes :

- *Mode de protection interactif.* Kaspersky Anti-Virus prévient l'utilisateur de tous les événements dangereux et suspects survenus dans le système. L'utilisateur doit lui-même prendre la décision d'autoriser ou d'interdire une action quelconque.
- *Mode de protection automatique.* Kaspersky Anti-Virus appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab lors d'événements dangereux.

➤ Pour utiliser le mode automatique de la protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Protection**.
3. Dans le groupe **Protection interactive** cochez la case ☒ **Sélectionner l'action automatiquement**. Si vous ne souhaitez pas que Kaspersky Anti-Virus supprime les objets suspects en mode automatique, cochez la case ☒ **Ne pas supprimer les objets suspects**.

RESTRICTION DE L'ACCES A KASPERSKY ANTI-VIRUS

Plusieurs personnes peuvent utiliser un même ordinateur et le niveau de connaissances informatiques de celles-ci varie. L'accès ouvert à Kaspersky Anti-Virus et à ces paramètres peut considérablement réduire le niveau de la protection globale de l'ordinateur.

Pour accroître la sécurité de l'ordinateur, définissez un mot de passe pour limiter l'accès à Kaspersky Anti-Virus. Vous pouvez bloquer n'importe quelle action de Kaspersky Anti-Virus, à l'exception des notifications en cas de découverte d'objets dangereux ou interdire l'une des actions suivantes :

- modification des paramètres de fonctionnement de l'application ;
- arrêt de l'application ;

➤ Pour protéger l'accès à Kaspersky Anti-Virus à l'aide d'un mot de passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Protection**.
3. Dans le groupe **Protection par mot de passe**, cochez la case ☒ **Activer la protection par mot de passe** puis cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Protection par un mot de passe** qui s'ouvre, saisissez le mot de passe et définissez le domaine d'application des restrictions. Désormais, chaque fois qu'un utilisateur de votre ordinateur tentera d'exécuter les actions de Kaspersky Anti-Virus que vous avez sélectionné, il devra saisir le mot de passe.

ANTIVIRUS FICHIERS

Cette fenêtre regroupe les paramètres du composant Antivirus Fichiers (cf. section "Protection du système de fichiers de l'ordinateur" à la page [42](#)). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- arrêter l'Antivirus Fichiers ;
- modifier le niveau de protection (cf. page [44](#)) ;
- modifier l'action à appliquer aux objets identifiés (cf. page [44](#)) ;
- constituer la couverture de protection (cf. page [45](#)) ;
- optimiser l'analyse (cf. page [46](#)) ;
- configurer l'analyse des fichiers composés (cf. page [47](#)) ;
- modifier le mode d'analyse (cf. page [48](#)) ;
- utiliser l'analyse heuristique (cf. page [46](#)) ;

- suspendre le composant (cf. page [49](#)) ;
- sélectionner la technologie d'analyse (cf. page [48](#)) ;
- restaurer les paramètres de protection par défaut (cf. page [51](#)), pour autant qu'ils aient été modifiés.

➡ *Pour désactiver l'utilisation de l'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, désélectionnez la case ☒ **Activer l'Antivirus Fichiers**.

➡ *Pour passer à la configuration des paramètres de l'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection et la réaction face à la menace pour le composant. Cliquez sur le bouton **Configuration** afin de passer à la configuration des autres paramètres d'Antivirus Fichiers.

ANTIVIRUS COURRIER

Cette fenêtre regroupe les paramètres du composant Antivirus Courrier (cf. section "Protection du courrier" à la page [52](#)). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- arrêter l'Antivirus Courrier ;
- modifier le niveau de protection (cf. page [53](#)) ;
- modifier l'action à appliquer aux objets identifiés (cf. page [54](#)) ;
- constituer la couverture de protection (cf. page [55](#)) ;
- utiliser l'analyse heuristique (cf. page [56](#)) ;
- configurer l'analyse des fichiers composés (cf. page [57](#)) ;
- configurer les règles de filtrage à appliquer aux pièces jointes (cf. page [57](#)) ;
- restaurer les paramètres de protection du courrier par défaut (cf. page [58](#)).

➡ *Pour désactiver l'utilisation de l'Antivirus Courrier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, cochez la case ☒ **Activer l'Antivirus Courrier**.

➡ *Pour passer à la configuration des paramètres de l'Antivirus Courrier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection et la réaction face à la menace pour le composant. Cliquez sur le bouton **Configuration** afin de passer à la configuration des autres paramètres d'Antivirus Courrier.

ANTIVIRUS INTERNET

Cette fenêtre regroupe les paramètres du composant Antivirus Internet (cf. section "Protection du trafic Internet" à la page 59). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- arrêter l'Antivirus Internet ;
- modifier le niveau de protection (cf. page 61) ;
- modifier l'action à appliquer aux objets identifiés (cf. page 61) ;
- constituer la couverture de protection (cf. page 62) ;
- modifier les méthodes d'analyse (cf. page 62) ;
- utiliser le module d'analyse des liens (cf. page 63) ;
- optimiser l'analyse (cf. page 64) ;
- utiliser l'analyse heuristique (cf. page 64) ;
- restaurer les paramètres de protection Internet par défaut (cf. page 65).

➡ *Pour désactiver l'utilisation de l'Antivirus Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection** sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, désélectionnez la case ☒ **Activer l'Antivirus Internet**.

➡ *Pour passer à la configuration des paramètres de l'Antivirus Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection** sélectionnez le composant **Antivirus Internet**.
3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection et la réaction face à la menace pour le composant. Cliquez sur le bouton **Configuration** afin de passer à la configuration des autres paramètres d'Antivirus Internet.

ANTIVIRUS IM ("CHAT")

Cette fenêtre regroupe les paramètres du composant Antivirus IM ("Chat") (cf. section "Protection du trafic des messageries instantanées" à la page [66](#)). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- désactiver l'Antivirus IM ("Chat") ;
- constituer la couverture de protection (cf. page [67](#)) ;
- modifier la méthode d'analyse (cf. page [67](#)) ;
- utiliser l'analyse heuristique (cf. page [68](#)).

➡ *Pour désactiver l'utilisation de l'Antivirus IM ("Chat"), procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, désélectionnez la case ☒ **Activer l'Antivirus IM ("Chat")**.

➡ *Pour passer à la configuration des paramètres de l'Antivirus IM, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, modifiez les paramètres du composant comme vous le souhaitez.

DEFENSE PROACTIVE

Cette fenêtre regroupe les paramètres du composant Défense Proactive. La modification des paramètres vous permet d'exécuter les opérations suivantes :

- désactiver la Défense proactive ;
- gérer la liste de l'activité dangereuse (cf. page [69](#)) ;
- modifier la réaction de l'application sur l'activité dangereuse dans le système (cf. page [70](#)) ;
- constituer un groupe d'applications de confiance (cf. page [71](#)) ;
- contrôler les comptes du système (cf. page [71](#)) ;

➡ *Pour désactiver l'utilisation de la Défense Proactive, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, désélectionnez la case ☒ **Activer la Défense Proactive**.

➡ Pour passer à la configuration des paramètres de la Défense Proactive, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, modifiez les paramètres du composant comme vous le souhaitez.

ANALYSE

L'ensemble de paramètres définis pour chaque tâche détermine le mode d'exécution de l'analyse des objets sur l'ordinateur.

Les experts de Kaspersky Lab ont élaboré des tâches d'analyse et de recherche de vulnérabilités. Les tâches de recherche d'éventuels virus sont :

- **Analyse des objets.** Analyse des objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet du système de fichiers de l'ordinateur.
- **Analyse Complète.** Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.
- **Analyse Rapide.** Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation.

La fenêtre de configuration de chaque tâche d'analyse vous permet de réaliser les opérations suivantes :

- sélectionner le niveau de protection pour l'exécution de la tâche ;
- sélectionner l'action qui sera exécutée en cas de découverte d'un objet infecté ou probablement infecté ;
- programmer le lancement automatique de la tâche.
- composer la liste des objets à analyser (pour les analyses complète et rapide) ;
- définir les types de fichiers soumis à l'analyse antivirus ;
- définir les paramètres d'analyse des fichiers composés ;
- sélectionner les méthodes et les technologies d'analyse ;

Vous pouvez, dans la section **Analyse**, indiquer les paramètres d'analyse automatique des disques amovibles lorsqu'ils sont connectés à l'ordinateur et créer des raccourcis pour le lancement rapide des tâches d'analyse et de recherche de vulnérabilités.

Dans la fenêtre de configuration de la tâche de recherche de vulnérabilités, vous pouvez :

- programmer le lancement automatique de la tâche.
- composer la liste des objets à analyser.

➡ Pour passer à la configuration des paramètres de la tâche, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des objets**, **Recherche de Vulnérabilités**).
3. Dans la partie droite de la fenêtre configurez les paramètres.

MISE A JOUR

La mise à jour de Kaspersky Anti-Virus s'opère conformément à la sélection de paramètres.

La fenêtre de configuration de la mise à jour vous permet de réaliser les opérations suivantes :

- modifier l'adresse de la ressource depuis laquelle les mises à jour de l'application seront copiées et installées ;
- indiquer le mode dans lequel la mise à jour de l'application sera lancée ;
- définir l'horaire de l'exécution de la tâche ;
- désigner le compte utilisateur sous lequel la mise à jour sera lancée ;
- indiquer les actions à exécuter après la mise à jour de l'application.

➡ Pour passer à la configuration des paramètres de la mise à jour, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans la partie droite de la fenêtre, indiquez le mode d'exécution requis et sélectionnez la source des mises à jour. Dans le groupe **Avancé**, définissez les autres paramètres de la tâche.

PARAMETRES

La fenêtre **Paramètres** vous permet d'utiliser les fonctions avancées suivantes de Kaspersky Anti-Virus :

- Autodéfense de Kaspersky Anti-Virus (cf. page [102](#)).
- Utilisation de la technologie de réparation de l'infection active (cf. page [103](#)).
- Service d'économie de la charge de la batterie (cf. page [103](#)).
- Exécution différée des tâches d'analyse en cas de ralentissement du fonctionnement des autres programmes (cf. page [104](#)).
- Exportation / importation des paramètres de fonctionnement de Kaspersky Anti-Virus (cf. page [104](#)).
- Restauration des paramètres de fonctionnement par défaut de Kaspersky Anti-Virus (cf. page [105](#)).

AUTODEFENSE DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus protège les ordinateurs contre les programmes malveillants et pour cette raison, il constitue une cible de choix pour les programmes malveillants qui tentent de le bloquer ou de le supprimer de l'ordinateur.

Pour garantir la stabilité du système de sécurité de votre ordinateur, Kaspersky Anti-Virus prévoit des mécanismes d'auto-défense et de protection contre les actions externes.

Sous les systèmes d'exploitation 64 bits et sous Microsoft Windows Vista, seule l'administration du mécanisme d'autodéfense de Kaspersky Anti-Virus contre la modification et la suppression des fichiers sur le disque ou des clés dans la base de registres est accessible.

Il arrive parfois que le recours à la protection contre les interventions à distance entraîne l'impossibilité d'utiliser les programmes d'administration à distance (par exemple, RemoteAdmin). Pour garantir leur fonctionnement, il faut ajouter ces applications à la liste des applications de confiance et activer le paramètre **Ne pas surveiller l'activité de l'application**.

➡ Pour enclencher l'utilisation des mécanismes d'autodéfense de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Autodéfense**, cochez la case ☒ **Activer l'autodéfense** pour activer le mécanisme de protection de Kaspersky Anti-Virus contre la modification ou la suppression de ces propres fichiers sur le disque, des processus en mémoire et des enregistrements dans la base de registre système.

Dans le groupe **Autodéfense**, cochez la case ☒ **Désactiver la possibilité d'administration externe du service système** pour bloquer toute tentative d'administration à distance des services de l'application.

Un message d'avertissement apparaîtra au-dessus de l'icône du programme dans la zone de notification de la barre des tâches en cas de tentative d'exécution des actions citées (pour autant que le service n'ait pas été désactivé par l'utilisateur).

TECHNOLOGIE DE REPARATION DES INFECTIONS ACTIVES

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. En cas de découverte d'une action malveillante dans le système, Kaspersky Anti-Virus propose la réalisation d'une procédure élargie de réparation qui permet de neutraliser la menace ou de la supprimer de l'ordinateur.

L'ordinateur redémarrera à la fin de la procédure. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète.

➡ Pour appliquer la procédure de réparation étendue, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Compatibilité**, cochez la case ☒ **Appliquer la technologie de désinfection avancée**.

FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS SUR UN ORDINATEUR PORTABLE

Afin d'économiser les batteries des ordinateurs portables, vous pouvez reporter les tâches liées à la recherche de virus.

Etant donné que la recherche de virus et la mise à jour sont assez gourmandes en ressources et durent un certain temps, nous vous conseillons de désactiver le lancement programmé de celles-ci. Cela vous permettra d'économiser la batterie. Au besoin, vous pourrez mettre à jour vous-même Kaspersky Anti-Virus ou lancer l'analyse antivirus.

➤ *Pour utiliser le mode d'économie de la batterie, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Compatibilité**, cochez la case ☒ **Ne pas lancer l'analyse programmée en cas d'alimentation via la batterie**.

PERFORMANCES DE L'ORDINATEUR PENDANT L'EXECUTION DES TACHES

Afin de limiter la charge appliquée au processeur central et aux sous-systèmes du disque, vous pouvez reporter les tâches liées à la recherche de virus.

L'exécution des tâches d'analyse augmente la charge du processeur central et des sous-systèmes du disque, ce qui ralentit le fonctionnement d'autres programmes. Lorsqu'une telle situation se présente, Kaspersky Anti-Virus arrête par défaut l'exécution des tâches d'analyse et libère des ressources pour l'application de l'utilisateur.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Pour que l'analyse ne dépende pas du fonctionnement de tels programmes, il ne faut pas leur céder des ressources.

Remarquez que ce paramètre peut être défini individuellement pour chaque tâche d'analyse. Dans ce cas, la configuration des paramètres pour une tâche particulière a une priorité supérieure.

➤ *Pour reporter l'exécution des tâches d'analyse en cas de ralentissement d'autres programmes, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Compatibilité** cochez la case ☒ **Céder les ressources aux autres applications**.

EXPORTATION/IMPORTATION DES PARAMETRES DE FONCTIONNEMENT DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus vous permet d'exporter ou d'importer ses paramètres.

Cela est utile si vous avez installé Kaspersky Anti-Virus sur un ordinateur chez vous et au bureau. Vous pouvez configurer le logiciel selon un mode qui vous convient pour le travail à domicile, conserver ces paramètres sur le disque et à l'aide de la fonction d'importation, les importer rapidement sur votre ordinateur au travail. Les paramètres sont enregistrés dans un fichier de configuration spécial.

➤ *Pour exporter les paramètres de fonctionnement actuel de Kaspersky Anti-Virus, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Administration des paramètres de l'application**, cliquez sur le bouton **Enregistrer**.
4. Saisissez le nom du fichier de configuration et précisez l'emplacement de la sauvegarde.

➤ Pour importer les paramètres de fonctionnement depuis le fichier de configuration, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Administration des paramètres de l'application**, cliquez sur le bouton **Importer**.
4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier à utiliser pour importer les paramètres de Kaspersky Anti-Virus.

RESTAURATION DES PARAMETRES PAR DEFAUT

Vous pouvez toujours revenir aux paramètres recommandés de Kaspersky Anti-Virus. Ces paramètres sont les paramètres optimaux recommandés par les experts de Kaspersky Lab. La restauration des paramètres est exécutée par l'Assistant de configuration initiale (cf. section "Assistant de configuration de l'application" à la page [26](#)) de l'application.

Dans la fenêtre qui s'affiche, vous aurez la possibilité de définir les paramètres et les composants pour lesquels vous souhaitez les conserver ou non en plus de la restauration du niveau de protection recommandé.

La liste propose les composants de Kaspersky Anti-Virus dont les paramètres ont été modifiés par l'utilisateur. Si des paramètres uniques ont été définis pour un composant quelconque, ils figureront également dans la liste.

Ces listes sont constituées pendant l'utilisation de Kaspersky Anti-Virus et tiennent compte des tâches individuelles et des exigences de sécurité. La constitution de telles listes prend en général beaucoup de temps et pour cette raison, nous vous recommandons de les conserver en cas de rétablissements des paramètres du programme à leur valeur d'origine.

Lorsque vous aurez quitté l'Assistant, tous les composants de la protection fonctionneront selon le niveau **Recommandé** et tiendront compte des paramètres que vous avez décidés de conserver lors de la restauration. De plus, les paramètres définis à l'aide de l'Assistant seront appliqués.

➤ Pour restaurer les paramètres de protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Administration des paramètres de l'application**, cliquez sur le bouton **Restaurer**.
4. Dans la fenêtre qui s'ouvre, cochez les cases pour les paramètres qui doivent être enregistrés. Cliquez sur **Suivant**. Cette action entraîne le lancement de l'Assistant de configuration initiale. Suivez les instructions affichées.

MENACES ET EXCLUSIONS

La section **Menaces et exclusions** de la fenêtre de configuration de Kaspersky Anti-Virus vous permet de réaliser les tâches suivantes

- Sélectionner les catégories de menaces identifiées (cf. section "Sélection des catégories de menaces identifiées" à la page [106](#)) ;
- composer la zone de confiance de l'application.

La *Zone de confiance* est en réalité une liste d'objets composée par l'utilisateur. Ces objets seront ignorés par l'application. En d'autres termes, il s'agit des éléments exclus de la protection offerte par Kaspersky Anti-Virus.

La zone de confiance se forme à la base de la liste des applications de confiance (cf. section "Sélection des applications de confiance" à la page [106](#)) et des règles d'exclusion (cf. section "Règles d'exclusion" à la page [107](#)).

L'utilisateur compose la zone de confiance en fonction des particularités des objets qu'il manipule et des programmes installés. La constitution de cette liste d'exclusions peut s'avérer utile si l'application bloque l'accès à un objet ou un programme quelconque alors que vous êtes convaincu que celui-ci est tout à fait sain.

VOIR EGALEMENT

Sélection des catégories de menaces identifiées	106
Sélection des applications de confiance.....	106
Règles d'exclusion	107
Masques autorisés pour l'exclusion des fichiers	108
Masques de types de menaces autorisés	109

SELECTION DES CATEGORIES DE MENACES IDENTIFIEES

Kaspersky Anti-Virus vous protège contre divers types d'applications malveillantes. Quels que soient les paramètres définis, l'application recherche toujours et neutralise les virus, les chevaux de Troie et les outils de pirates informatiques. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Afin de garantir une protection plus étendue, vous pouvez agrandir la liste des menaces à découvrir en activant la recherche de divers programmes qui présentent un risque potentiel.

➡ *Pour sélectionner les catégories de menaces à identifier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Menaces et exclusions**. Cliquez sur le bouton **Configuration** dans le groupe **Menaces**.
3. Dans la fenêtre **Menaces** qui s'ouvre, sélectionnez les catégories de menaces contre lesquelles vous souhaitez protéger votre ordinateur.

SELECTION DES APPLICATIONS DE CONFIANCE

Vous pouvez composer une liste d'applications de confiance dont l'activité au niveau des fichiers et du réseau (y compris toute activité suspecte) ou les requêtes envoyées à la base de registres système ne seront plus contrôlées.

Par exemple, vous estimez que les objets utilisés par le programme Bloc-notes de Microsoft Windows sont inoffensifs et n'ont pas besoin d'être analysés. En d'autres termes, vous faites confiance aux processus de ce programme. Afin d'exclure de l'analyse les objets utilisés par ce processus, ajoutez le programme Bloc-notes à la liste des applications de confiance. Le fichier exécutable et le processus de l'application de confiance seront toujours soumis à la recherche de virus. Pour exclure entièrement l'application de l'analyse, il faut recourir aux règles d'exclusion.

De plus, certaines actions jugées dangereuses peuvent être tout à fait normales dans le cadre du fonctionnement de toute une série de programmes. Ainsi, l'interception des frappes au clavier est une action standard pour les programmes de permutation automatique de la disposition du clavier (Punto Switcher, etc.). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

Le recours aux exclusions d'applications de confiance de l'analyse permet de résoudre les éventuels problèmes de compatibilité entre Kaspersky Anti-Virus et d'autres applications (par exemple, le problème de la double analyse du trafic de réseau d'un ordinateur tiers par Kaspersky Anti-Virus et une autre application antivirus) et d'augmenter les performances de l'ordinateur ce qui est particulièrement important en cas d'utilisation d'applications de réseau.

Par défaut Kaspersky Anti-Virus analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère.

➤ Pour ajouter une application à la liste des applications de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Menaces et exclusions**.
3. Dans la rubrique **Exclusions**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Applications de confiance** cliquez sur le lien **Ajouter**.
5. Sélectionnez l'application dans le menu qui s'ouvre. Si vous sélectionnez **Parcourir**, vous ouvrirez une fenêtre dans laquelle vous devrez saisir le chemin d'accès au fichier exécutable. Si vous sélectionnez **Applications**, vous ouvrirez la liste des applications en cours d'exécution.
6. Dans la fenêtre **Exclusions pour l'application** qui s'ouvre, définissez les paramètres des règles pour l'application.

Vous pouvez modifier ou supprimer l'application de confiance de la liste à l'aide des liens du même nom situé dans la partie inférieure de l'onglet. Pour exclure l'application de la liste sans toutefois la supprimer, décochez la case en regard de cette dernière.

REGLES D'EXCLUSION

Les applications qui présentent un danger potentiel n'ont aucune fonction malveillante mais elles peuvent être utilisées en tant qu'élément qui va aider un programme malveillant car elles contiennent des failles et des erreurs. Cette catégorie reprend les programmes d'administration à distance, les clients IRC, les serveurs FTP, les utilitaires d'arrêt des processus ou de dissimulation de ceux-ci, les enregistreurs de frappe de clavier, les programmes de décodage des mots de passe, les numéroteurs automatiques vers des numéros payants, etc. Ce genre d'application n'est pas considéré comme un virus (not-a-virus). Il peut s'agir d'un programme de type Adware, Joke, Riskware, etc. (pour obtenir de plus amples informations sur les applications malveillantes découvertes par l'application, consultez l'encyclopédie des virus à l'adresse www.viruslist.com/fr). Ces programmes peuvent être bloqués suite à l'analyse. Dans la mesure où l'utilisation de certains d'entre eux est très populaire, il est prévu de pouvoir les exclure de l'analyse.

Admettons que vous utilisiez souvent Remote Administrator. Il s'agit d'une application d'accès à distance qui permet de travailler sur un ordinateur distant. L'activité générée par cette application est considérée comme potentiellement dangereuse par Kaspersky Anti-Virus et peut être bloquée. Pour exclure le blocage de l'application, il faut créer une règle d'exclusion pour l'application qui la reconnaît comme *not-a-virus:RemoteAdmin.Win32.RAdmin.22* conformément à l'Encyclopédie des virus.

La *règle d'exclusion* est un ensemble de conditions qui, si elles sont vérifiées, entraîne l'exclusion de l'objet de l'analyse réalisée par Kaspersky Anti-Virus.

Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple : un répertoire ou un programme), des processus ou des objets selon un type de menace conforme à la classification de l'encyclopédie des virus.

Le *type de menace* est l'état attribué à l'objet par Kaspersky Anti-Virus lors de l'analyse. Le type de menace est rendu sur la base du classement des programmes malveillants et des riskwares présentés dans l'encyclopédie des virus de Kaspersky Lab.

Lorsqu'une règle est ajoutée, une règle est créée. Celle-ci pourra être utilisée par la suite par certains composants de l'application (par exemple, l'Antivirus Fichiers (cf. section "Protection du système de fichiers de l'ordinateur" à la page 42), l'Antivirus Courrier (cf. section "Protection du courrier" à la page 52), l'Antivirus Internet (cf. section "Protection du trafic Internet" à la page 59)), ainsi que lors de l'exécution des tâches d'analyse.

➤ Pour créer une règle d'exclusion, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Menaces et exclusions**.

3. Dans la rubrique **Exclusions**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles d'exclusion**, cliquez sur le lien **Ajouter**.
5. Dans la fenêtre **Règle d'exclusion** qui s'ouvre, définissez les paramètres des règles d'exclusion.

VOIR EGALEMENT

Masques autorisés pour l'exclusion des fichiers [108](#)

Masques de types de menaces autorisés [109](#)

MASQUES AUTORISÉS POUR L'EXCLUSION DES FICHIERS

Voici des exemples de masques autorisés que vous pouvez utiliser dans la composition de la liste des fichiers à exclure. Parmi ceux-ci, citons les éléments suivants :

1. Masques sans chemins d'accès aux fichiers :
 - ***.exe** : tous les fichiers avec extension **exe** ;
 - **tous les fichiers *.exe** : tous les fichiers avec extension **ex?**, où **?** peut représenter tout caractère singulier ;
 - **test** : tous les fichiers avec le nom **test**.
2. Masques avec chemins d'accès absolus aux fichiers :
 - **C:\dir*.*** ou **C:\dir*** ou **C:\dir** : tous les fichiers du répertoire **C:\dir** ;
 - **C:\dir*.exe** : tous les fichiers avec l'extension **exe** dans le répertoire **C:\dir** ;
 - **C:\dir*.ex?** : tous les fichiers portant l'extension **ex?** dans le répertoire **C:\dir**, où **?** peut représenter n'importe quel caractère unique ;
 - **C:\dir\test** : uniquement le fichier **C:\dir\test**.

Afin de ne pas analyser les fichiers dans tous les sous-répertoires du répertoire indiqué, désélectionnez la case ☒ **Sous-répertoire compris** lors de la définition du masque.
3. Masques de chemins d'accès aux fichiers :
 - **dir*.*** ou **dir*** ou **dir** : tous les fichiers dans tous les répertoires **dir** ;
 - **dir\test** : tous les fichiers **test** dans les répertoires **dir** ;
 - **dir*.exe** : tous les fichiers portant l'extension **exe** dans tous les répertoires **dir** ;
 - **dir*.ex?** : tous les fichiers portant l'extension **ex?** dans tous les répertoires **dir**, où **?** peut représenter tout caractère singulier.

Afin de ne pas analyser les fichiers dans tous les sous-répertoires du répertoire indiqué, désélectionnez la case ☒ **Sous-répertoire compris** lors de la définition du masque.

L'utilisation des masques d'exclusion *.* ou * est admissible uniquement lors de l'indication de la classification des menaces exclues selon l'Encyclopédie des virus. Dans ce cas, la menace indiquée ne sera pas décelée dans tous les objets. L'utilisation de ces masques sans indication de la classification revient à désactiver la protection. Aussi, il n'est pas recommandé de sélectionner, en tant qu'exclusion, le chemin d'accès appartenant au disque virtuel, généré sur la base du catalogue du système de fichiers par l'instruction subst, ou le disque qui est l'image du répertoire de réseau. Il se fait que pour divers utilisateurs d'un ordinateur, le même nom de disque peut désigner différentes ressources, ce qui entraîne inévitablement un dysfonctionnement de la règle d'exclusion.

MASQUES DE TYPES DE MENACES AUTORISEES

Pour ajouter des menaces d'un verdict particulier (conforme au classement de l'encyclopédie des virus) en guise d'exclusion, vous pouvez indiquer les paramètres suivants :

- le nom complet de la menace, tel que repris dans l'Encyclopédie des virus sur <http://www.viruslist.com/fr> (ex. *not-a-virus:RiskWare.RemoteAdmin.RA.311* ou *Flooder.Win32.Fuxx*);
- Le nom de la menace selon un masque, par exemple :
 - **not-a-virus*** : exclut de l'analyse les logiciels licites mais potentiellement dangereux, ainsi que les jokewares ;
 - ***Riskware.*** : exclut de l'analyse tous les types de logiciels présentant un risque potentiel de type Riskware ;
 - ***RemoteAdmin.*** : exclut de l'analyse toutes les versions de logiciel d'administration à distance.

RESEAU

La section **Réseau** de la fenêtre de configuration de l'application vous permet de sélectionner les ports contrôlés par Kaspersky Anti-Virus et de configurer l'analyse des connexions sécurisées :

- composer la liste des ports contrôlés ;
- activer / désactiver le mode d'analyse des connexions sécurisées (via le protocole SSL) (cf. page [110](#)) ;
- configurer les paramètres du serveur proxy (cf. page [112](#)).

VOIR EGALEMENT

Constitution de la liste des ports contrôlés	109
Analyse des connexions sécurisées	110
Analyse des connexions sécurisées dans Mozilla Firefox	111
Analyse des connexions sécurisées dans Opera.....	112
Paramètres du serveur proxy	112

CONSTITUTION DE LA LISTE DES PORTS CONTROLES

Les composants de la protection tels que l'Antivirus Courrier (cf. section "Protection du courrier" à la page [52](#)) et l'Antivirus Internet (cf. section "Protection du trafic Internet" à la page [59](#)) contrôlent les flux de données transmis par des protocoles définis et qui transitent par certains ports ouverts de l'ordinateur. Ainsi, l'Antivirus Courrier analyse les données transmises via le protocole SMTP tandis que l'Antivirus Internet analyse les paquets HTTP.

Vous avez le choix entre deux modes de contrôle des ports :

-  **Contrôler tous les ports de réseau ;**
-  **Contrôler uniquement les ports sélectionnés.** La liste des ports qui sont normalement utilisés pour le courrier et le trafic http sont repris dans le logiciel.

➤ *Pour ajouter un port à la liste des ports contrôlés, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans le bloc **Ports contrôlés**, cliquez sur **Sélection**.
4. Dans la fenêtre **Ports de réseau** qui s'ouvre, cliquez sur le lien **Ajouter**.
5. Dans la fenêtre **Port de réseau** qui s'ouvre, saisissez les données requises.

➤ *Pour exclure un port de la liste des ports contrôlés, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans le bloc **Ports contrôlés**, cliquez sur **Sélection**.
4. Dans la fenêtre **Ports de réseau** qui s'ouvre, décochez la case ☒ en regard de la description du port.

➤ *Pour former la liste des applications dont l'ensemble des ports devra être analysé, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans le bloc **Ports contrôlés**, cliquez sur **Sélection**.
4. Dans la fenêtre **Ports de réseau** qui s'ouvre, cochez la case ☒ **Contrôler tous les ports pour les applications indiquées** puis cliquez sur le lien **Ajouter** dans le groupe du dessous.
5. Sélectionnez l'application dans le menu qui s'ouvre. Si vous sélectionnez **Parcourir**, vous ouvrirez une fenêtre dans laquelle vous devrez saisir le chemin d'accès au fichier exécutable. Si vous sélectionnez **Applications**, vous ouvrirez la liste des applications en cours d'exécution.
6. Dans la fenêtre **Application** qui s'ouvre, saisissez une description pour l'application sélectionnée.

ANALYSE DES CONNEXIONS SECURISEES

Les connexions à l'aide du protocole SSL protègent le canal d'échange des données sur Internet. Le protocole SSL permet d'identifier les parties qui échangent les données sur la base de certificats électroniques, de crypter les données transmises et de garantir leur intégrité tout au long de la transmission.

Ces particularités du protocole sont exploitées par les individus mal intentionnés afin de diffuser leurs logiciels malveillants car la majorité des logiciels antivirus n'analyse pas le trafic SSL.

Kaspersky Anti-Virus analyse les connexions sécurisées à l'aide d'un certificat de Kaspersky Lab. Ce certificat sera toujours utilisé pour l'analyse de la sécurité de la connexion.

Par la suite, l'analyse du trafic SSL aura lieu à l'aide du certificat de Kaspersky Lab. Si un certificat non valide est découvert au moment d'établir la connexion avec le serveur (par exemple, il a été remplacé par un individu mal intentionné), un message s'affichera et invitera l'utilisateur à accepter ou non le certificat ou à consulter les informations relatives à ce dernier. Si l'application fonctionne en mode automatique, la connexion qui utilise le certificat incorrect sera coupée sans notification.

➤ *Pour activer l'analyse des connexions sécurisées, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans la fenêtre qui s'ouvre, cochez la case ☒ **Analyse des connexions sécurisées** puis cliquez sur le bouton **Installer le certificat**.
4. Dans la fenêtre qui s'affiche, cliquez sur **Installer le certificat**. Cela lancera l'Assistant. Suivez ses instructions pour l'installation du certificat.

L'installation automatique du certificat a lieu uniquement lors de l'utilisation de Microsoft Internet Explorer. Pour l'analyse des connexions sécurisées dans Mozilla Firefox et Opera, installez le certificat de Kaspersky Lab manuellement.

ANALYSE DES CONNEXIONS SECURISEES DANS MOZILLA FIREFOX

Le navigateur Mozilla Firefox n'utilise pas le référentiel de certificats de Microsoft Windows. Pour analyser les connexions sécurisées à l'aide de Firefox, il faut installer manuellement le certificat de Kaspersky Lab.

➤ *Pour installer le certificat de Kaspersky Lab, procédez comme suit :*

1. Dans le menu du navigateur, sélectionnez le point **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Dans le bloc **Certificats**, sélectionnez l'onglet **Sécurité** et cliquez sur **Consultation des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certifications** puis cliquez sur le bouton **Restaurer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer`
6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur le bouton **Consulter**.

➤ *Pour installer le certificat de Kaspersky Lab pour Mozilla Firefox version 3.x, procédez comme suit :*

1. Dans le menu du navigateur, sélectionnez le point **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Sous l'onglet **Cryptage** cliquez sur **Consultation des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certifications** puis cliquez sur le bouton **Importer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer`

6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur **Voir**.

Si votre ordinateur fonctionne sous le système d'exploitation Microsoft Windows Vista, alors le chemin d'accès au fichier du certificat de Kaspersky Lab sera : %AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.

ANALYSE DES CONNEXIONS SECURISEES DANS OPERA

Le navigateur Opera n'utilise pas le référentiel de certificats de Microsoft Windows. Pour analyser les connexions sécurisées à l'aide d'Opera, il faut installer manuellement le certificat de Kaspersky Lab.

➤ *Pour installer le certificat de Kaspersky Lab, procédez comme suit :*

1. Dans le menu du navigateur, sélectionnez le point **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Editeurs** puis cliquez sur le bouton **Importer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.
6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé. Pour consulter les informations relatives au certificat et pour sélectionner les actions qui utiliseront le certificat, sélectionnez le certificat dans la liste et cliquez sur le bouton **Consulter**.

➤ *Pour installer le certificat de Kaspersky Lab pour Opera version 9.x, procédez comme suit :*

1. Dans le menu du navigateur, sélectionnez le point **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certifications** puis cliquez sur le bouton **Importer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :
%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.
6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé.

Si votre ordinateur fonctionne sous le système d'exploitation Microsoft Windows Vista, alors le chemin d'accès au fichier du certificat de Kaspersky Lab sera : %AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.

PARAMETRES DU SERVEUR PROXY

Si la connexion à Internet s'opère via un serveur proxy, il faudra alors peut-être configurer les paramètres de connexion à ce dernier. Kaspersky Anti-Virus applique ces paramètres dans quelques composants de la protection ainsi que dans la mise à jour des bases et des modules de l'application.

Si votre réseau est doté d'un serveur proxy qui utilise un port inhabituel, il faudra l'ajouter à la liste des ports contrôlés.

➡ *Pour configurer les paramètres du serveur proxy, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans le groupe **Serveur proxy**, cliquez sur le bouton **Paramètres du serveur proxy**.
4. Dans la fenêtre **Paramètres du serveur proxy** qui s'ouvre, modifiez les paramètres du serveur proxy.

NOTIFICATIONS

Divers événements peuvent survenir pendant le fonctionnement de Kaspersky Anti-Virus. Elles peuvent avoir un caractère purement informatif ou présenter des informations cruciales. Par exemple, la notification peut signaler la réussite de la mise à jour ou signaler une erreur dans le fonctionnement d'un composant qu'il faudra rectifier au plus vite.

Pour rester au courant des événements qui surviennent dans le fonctionnement de Kaspersky Anti-Virus, utilisez le service de notifications.

Par défaut, l'utilisateur est prévenu à l'aide de fenêtres contextuelles et de signaux sonores.

La notification peut être réalisée de l'une des manières suivantes :

- messages contextuels au-dessus de l'icône de l'application dans la barre des tâches ;
- notification sonore ;
- messages électroniques.

➡ *Afin de désactiver la remise des notifications, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Notifications**.
3. Décochez la case ☒ **Notifier les événements**.

Même si l'affichage de la notification est désactivé, les informations relatives aux événements qui surviennent pendant l'utilisation de Kaspersky Anti-Virus seront consignées dans le Rapports sur l'activité de l'application.

➡ *Afin de désactiver le moyen de remise des notifications, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Notifications** puis cliquez sur le bouton **Configuration**.
3. Dans la fenêtre **Notification** qui s'ouvre, sélectionnez le mode de notification.

VOIR EGALEMENT

Désactivation de la sonorisation des notifications	114
Envoi des notifications à l'aide du courrier électronique	114

DESACTIVATION DE LA SONORISATION DES NOTIFICATIONS

Par défaut, toutes les notifications sont accompagnées d'un son. Ces sons proviennent de Microsoft Windows. La case ☒ **Utiliser les sons standards de Windows par défaut** permet de modifier la sélection de sons utilisée. Si la case est décochée, c'est la sélection de sons de la version antérieure de l'application qui sera utilisée.

➤ *Pour désactiver l'accompagnement sonore, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Notifications**.
3. Décochez la case ☒ **Activer les sons des notifications**.

ENVOI DES NOTIFICATIONS A L'AIDE DU COURRIER ELECTRONIQUE

Si vous choisissez de recevoir les notifications par courrier électronique, il faudra définir les paramètres de livraison.

➤ *Pour configurer les paramètres du courrier électronique pour l'envoi des notifications, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Notifications**.
3. Cochez la case ☒ **Activer les notifications par courriers** puis cliquez sur le bouton **Configuration e-mail**.
4. Dans la fenêtre **Configuration des notifications par courrier** qui s'ouvre définissez les paramètres de livraison.

RAPPORTS ET STOCKAGES

La rubrique reprend les paramètres qui régissent l'utilisation des fichiers de données de Kaspersky Anti-Virus.

Les fichiers de données de l'application sont les objets placés en quarantaine ou dans la sauvegarde pendant l'utilisation de Kaspersky Anti-Virus ainsi que les fichiers des rapports sur le fonctionnement des composants de l'application.

Dans cette section, vous pouvez :

- configurer les paramètres de création (cf. page [115](#)) et de conservation des rapports (cf. page [115](#)) ;
- configurer les paramètres de la quarantaine et du dossier de sauvegarde (cf. page [117](#)).

VOIR EGALEMENT

Ajout d'enregistrements relatifs aux événements dans le rapport	115
Purge des rapports	115
Conservation des rapports	115
Quarantaine pour les objets potentiellement infectés.....	116
Copie de sauvegarde des objets dangereux	116
Manipulation des objets en quarantaine.....	117
Conservation des objets de la quarantaine et de la sauvegarde.....	117
Rapports.....	127

AJOUT D'ENREGISTREMENTS RELATIFS AUX EVENEMENTS DANS LE RAPPORT

Vous pouvez ajouter au rapport de la protection des enregistrements sur les événements non critiques ou sur les événements de la base de registres et du système de fichiers. Ces enregistrements ne sont pas ajoutés par défaut.

- *Pour ajouter au rapport des enregistrements sur les événements non critiques, sur les événements de la base de registres et / ou du système de fichiers, procédez comme suit :*
1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
 2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Rapports et Stockages**.
 3. Dans le groupe **Rapports**, cochez la case ☒ requise.

PURGE DES RAPPORTS

Les informations relatives au fonctionnement de Kaspersky Anti-Virus sont consignées dans les rapports. Vous pouvez les purger.

- *Pour purger les rapports, procédez comme suit :*
1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
 2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Rapports et Stockages**.
 3. Dans le bloc **Rapports** cliquez sur **Purger**.
 4. Dans la fenêtre **Suppression des informations des rapports**, cochez les cases en regard des catégories de rapports que vous souhaitez purger.

CONSERVATION DES RAPPORTS

Vous pouvez définir la durée maximale de conservation des rapports des événements (case ☒ **Supprimer les rapports après**). Par défaut, cette valeur est égale à 30 jours. Une fois ce délai écoulé, les objets sont supprimés. La durée maximale de conservation peut être modifiée, voire complètement annulée. Il est également possible de définir la taille

maximale du fichier du journal (case ☒ **Taille maximale de fichier**). Par défaut, la taille maximale est limitée à 1024 Mo. Une fois que la taille maximale est atteinte, le contenu du fichier est remplacé par de nouveaux enregistrements. Vous pouvez supprimer les restrictions sur la taille du rapport ou attribuer une autre valeur.

➤ *Afin de configurer les paramètres de conservation des rapports, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Rapports et Stockages**.
3. Dans la fenêtre qui s'ouvre, dans le groupe **Rapports**, cochez les cases requises ☒ et, le cas échéant, modifiez la taille maximale du journal et la durée de conservation.

QUARANTAINE POUR LES OBJETS POTENTIELLEMENT INFECTES

La *quarantaine* est un dossier spécial dans lequel on retrouve les objets qui ont peut-être été infectés par des virus.

Les objets potentiellement infectés sont des objets qui ont peut-être été infectés par des virus ou leur modification.

L'objet potentiellement infecté peut-être identifié et mis en quarantaine par l'Antivirus Fichiers, l'Antivirus Courrier, lors de l'analyse antivirus ou par la Défense Proactive.

Les objets sont placés en quarantaine suite aux actions de l'Antivirus Fichiers ou de l'Antivirus Courrier ainsi qu'après l'analyse si :

- *Le code de l'objet analysé est semblable à celui d'une menace connue mais a été partiellement modifié.*

Les bases de Kaspersky Anti-Virus contiennent les menaces qui ont été étudiées par les experts de Kaspersky Lab. Si le programme malveillant a été modifié et que ces modifications ne figurent pas encore dans les bases, Kaspersky Anti-Virus considère l'objet comme étant infecté par une modification d'un programme malveillant et le classe comme objet potentiellement infecté. Il indique obligatoirement à quelle menace cette infection ressemble.

- *Le code de l'objet infecté rappelle, par sa structure, celui d'un programme malveillant mais les bases de l'application ne recensent rien de similaire.*

Il est tout à fait possible qu'il s'agisse d'un nouveau type de virus et pour cette raison, Kaspersky Anti-Virus le classe comme un objet potentiellement infecté.

L'analyseur heuristique de code détermine si un fichier est potentiellement infecté par un virus. Ce mécanisme est assez efficace et entraîne rarement des faux-positifs.

S'agissant de la Défense Proactive, le composant met l'objet en quarantaine si l'analyse de la séquence d'actions qu'il réalise suscite des doutes.

Dans ce cas, l'objet est déplacé et non pas copié : l'objet est supprimé du disque ou du message et il est enregistré dans le répertoire de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

Après la mise à jour des bases de l'application, il se peut que Kaspersky Anti-Virus puisse identifier la menace et la neutraliser. C'est pour cette raison que le logiciel analyse les objets en quarantaine après chaque mise à jour (cf. page [91](#)).

COPIE DE SAUVEGARDE DES OBJETS DANGEREUX

Il n'est pas toujours possible de préserver l'intégrité des objets lors de la réparation. Si le fichier réparé contenait des informations importantes et que celles-ci ne sont plus accessibles (complètement ou partiellement) suite à la réparation, il est possible de tenter de le restaurer au départ de sa copie de sauvegarde.

La *copie de sauvegarde* est une copie de l'objet dangereux original qui est créée lors de la première réparation ou suppression de l'objet en question et qui est conservée dans le dossier de sauvegarde.

Le *dossier de sauvegarde* est un dossier spécial qui contient les copies des objets dangereux traités ou supprimés. La principale fonction de la sauvegarde est de garantir la possibilité de restaurer l'objet original à n'importe quel moment. Les fichiers placés dans le dossier de sauvegarde sont convertis dans un format spécial et ne représentent aucun danger.

MANIPULATION DES OBJETS EN QUARANTAINE

Vous pouvez réaliser les opérations suivantes sur les objets en quarantaine :

- mettre en quarantaine les fichiers qui selon vous sont infectés par un virus ;
- analyser et réparer à l'aide de la version actuelle des bases de Kaspersky Anti-Virus tous les objets potentiellement infectés qui se trouvent en quarantaine ;
- restaurer les fichiers dans un répertoire choisi par l'utilisateur ou dans le répertoire d'origine où ils se trouvaient avant d'être mis en quarantaine ;
- supprimer n'importe quel objet ou groupe d'objets de la quarantaine ;
- envoyer un objet de la quarantaine à Kaspersky Lab pour étude.

➡ Pour réaliser une action quelconque sur les objets en quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Quarantaine**.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces détectées** exécutez les actions requises.

CONSERVATION DES OBJETS DE LA QUARANTAINE ET DE LA SAUVEGARDE.

Vous pouvez configurer les paramètres suivants de fonctionnement de la quarantaine et de la sauvegarde :

- Définir la durée de conservation maximum des objets en quarantaine et des copies des objets dans le dossier de sauvegarde (la case ☒ **Supprimer les objets après**). Par défaut, la durée de conservation des objets est 30 jours, après lesquels ils seront supprimés. Vous pouvez modifier la durée de conservation maximum des rapports ou ne pas imposer de limite.
- Indiquer la taille maximale de la quarantaine (case ☒ **Taille maximale**). Par défaut, la taille maximale est limitée à 100 Mo. Vous pouvez supprimer les restrictions sur la taille du rapport ou attribuer une autre valeur.

➡ Pour configurer les paramètres de la quarantaine ou de la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Rapports et Stockages**.
3. Dans le groupe **Quarantaine et sauvegarde**, cochez les cases requises et, le cas échéant, indiquez la taille maximale du dossier où seront conservées les données.

KASPERSKY SECURITY NETWORK

Chaque jour dans le monde, une multitude de nouveaux virus apparaissent. Pour accélérer la collecte de données statistiques sur les types de nouvelles menaces et leurs sources ainsi que dans le but de les neutraliser, Kaspersky Lab vous offre la possibilité d'utiliser les services du *Kaspersky Security Network*.

Le service Kaspersky Security Network suppose l'envoi à Kaspersky Lab de certaines informations. Les informations suivantes sont transmises :

- L'identifiant unique attribué à votre ordinateur par l'application de Kaspersky Lab. Cet identifiant définit les paramètres matériels de votre ordinateur et ne contient aucune donnée personnelle.
- Les informations relatives aux menaces découvertes par les composants du programme. Le contenu de ces informations dépend du type de menace identifiée.
- Les informations relatives au système : version du système d'exploitation, mises à jour installées, services et pilotes téléchargés, version des navigateurs et des clients de messagerie, modules externes des navigateurs, numéro de la version de l'application de Kaspersky Lab installée.

➡ Pour activer l'envoi des statistiques dans Kaspersky Security Network, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Kaspersky Security Network**.
3. Cochez la case ☒ **J'accepte de rejoindre le Kaspersky Security Network**.

ASPECT EXTERIEUR DU RAPPORT

Vous pouvez également modifier l'apparence de l'application en créant et en utilisant diverses éléments graphiques et la palette de couleurs. Il est aussi possible de configurer l'utilisation des éléments actifs de l'interface (icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows et messages contextuels).

VOIR EGALEMENT

Eléments actifs de l'interface	118
Présentation graphique de Kaspersky Anti-Virus.....	119

ELEMENTS ACTIFS DE L'INTERFACE

Pour configurer les éléments actifs de l'interface (par exemple, icône de Kaspersky Anti-Virus dans la barre des tâches et messages contextuels), vous pouvez exploiter les possibilités suivantes de Kaspersky Anti-Virus.

Animer l'icône durant l'exécution des tâches.

L'aspect de l'icône change en fonction de l'opération exécutée par l'opération. Ainsi, lors de l'analyse d'un script, un pictogramme avec un script apparaît sur le fond de l'icône tandis qu'un pictogramme représentant un message apparaît pendant l'analyse d'un message. L'icône de Kaspersky Anti-Virus est animée. Dans ce cas, elle représentera uniquement l'état de la protection de votre ordinateur : si la protection est activée, l'icône sera en couleur. Si la protection est suspendue ou désactivée, l'icône sera grise.

Utiliser la transparence pour les fenêtres de notification.

Toutes les opérations de l'application qui requièrent une notification ou une prise de décision immédiate sont présentées dans un message contextuel qui apparaît au-dessus de l'icône de l'application dans la barre des tâches. Ces infobulles sont transparentes afin de ne pas vous perturber dans votre travail. Le fond de la fenêtre devient solide lorsque le curseur est déplacé sur celle-ci.

M'avertir des informations de Kaspersky Lab.

Par défaut, quand des informations sont obtenues, une icône spéciale apparaît dans la barre d'état. Il suffit de cliquer sur cette icône pour ouvrir une fenêtre contenant le texte des informations.

Afficher "Protected by Kaspersky Lab" sur l'écran de bienvenue de Microsoft Windows.

Cet indicateur apparaît par défaut dans le coin supérieur gauche de l'écran au lancement de Kaspersky Anti-Virus. Il indique que votre ordinateur est protégé contre tout type de menace.

Si le programme est installé sur un ordinateur fonctionnant sous Microsoft Windows Vista, cette possibilité ne sera pas offerte.

➤ Pour configurer les éléments actifs de l'interface, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Apparence**.
3. Dans le groupe **Icône de la barre des tâches**, cochez ou décochez les cases correspondantes .

PRESENTATION GRAPHIQUE DE KASPERSKY ANTI-VIRUS

Toutes les couleurs, polices de caractères, images et textes utilisés dans l'interface de Kaspersky Anti-Virus peuvent être modifiés. Vous pouvez créer votre propre environnement graphique pour le logiciel et localiser l'interface dans la langue de votre choix.

➤ Pour sélectionner un autre skin, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Apparence**.
3. Dans le groupe **Skins**, cochez la case  **Utiliser un skin personnalisé** pour associer un skin. Dans le champ, saisissez le répertoire contenant les paramètres des thèmes. Cliquez sur **Parcourir** pour sélectionner le répertoire.

UTILISATION DES PROFILS DE KASPERSKY ANTI-VIRUS

L'utilisation de certaines applications (par exemple, des jeux) en mode plein écran entraîne la nécessité de désactiver certaines fonctions de Kaspersky Anti-Virus, en particulier le service de notifications. Ces applications requièrent également une grande quantité de ressources système et par conséquent, l'exécution de certaines tâches de Kaspersky Anti-Virus peut ralentir leur fonctionnement.

Afin de ne pas devoir désactiver les notifications et suspendre les tâches manuellement à chaque fois lors d'utilisation d'applications en mode plein écran, il est possible de modifier temporairement les paramètres de Kaspersky Anti-Virus grâce au mode jeu. Le Mode Jeux permet de modifier simultanément les paramètres de tous les composants lors du passage en mode plein écran et de remettre à l'état antérieur les modifications apportées après y avoir quitté.

Lors du passage en mode plein écran, les notifications sur les événements sont désactivées automatiquement. Outre cela, vous pouvez spécifier les paramètres suivants :

-  **Sélectionner l'action automatiquement.** Si ce paramètre est sélectionné, alors, en tant que réaction, la sélection automatique de l'action sera appliquée pour tous les composants, même si dans leurs paramètres l'option  **Confirmer l'action** est sélectionnée. Ce faisant, l'utilisateur ne va pas recevoir de propositions sur la sélection de l'action sur les menaces détectées, et l'application choisira l'action automatiquement.
-  **Ne pas exécuter la mise à jour** et  **Ne pas réaliser les analyses programmées.** L'utilisation de ces paramètres est recommandée pour éviter le ralentissement des applications en mode plein écran.

➡ *Pour activer l'utilisation du Mode Jeux, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Mode Jeux**.
3. Cochez la case ☒ **Activer le Mode Jeux** et saisissez les paramètres nécessaires.

POSSIBILITES COMPLEMENTAIRES

Garantir la protection de l'ordinateur est une tâche complexe qui requiert des connaissances sur les particularités de fonctionnement du système d'exploitation et sur les moyens d'exploiter ses points faibles. De plus, le volume important des informations sur la protection du système et la diversité de celles-ci complique l'analyse et le traitement.

Pour faciliter l'exécution de tâches spécifiques pour la sécurité de l'ordinateur, Kaspersky Anti-Virus contient plusieurs assistants et outils :

- Le Clavier virtuel (cf. page [121](#)) qui permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.
- L'Assistant de création de disque de dépannage (cf. page [122](#)) qui rétablit le fonctionnement du système après une attaque de virus si les fichiers système du système d'exploitation ont été endommagés et que celui-ci ne peut être chargé.
- L'Assistant de configuration du navigateur (cf. page [124](#)) qui analyse les paramètres du navigateur Microsoft Internet Explorer et qui les évalue avant tout du point de vue de la sécurité.
- L'Assistant de restauration après infection (cf. page [125](#)) permet de liquider les traces de la présence d'objets malveillants dans le système.
- L'Assistant de suppression des traces d'activité (cf. page [126](#)) qui permet de retrouver et d'éliminer les traces d'activité de l'utilisateur dans le système.

DANS CETTE SECTION

Clavier virtuel.....	121
Disque de dépannage	122
Configuration du navigateur	124
Restauration après infection	125
Assistant de suppression des traces d'activité.....	126

CLAVIER VIRTUEL

Au cours de l'utilisation de l'ordinateur, il arrive souvent qu'il faille saisir des données personnelles ou un nom d'utilisateur et un mot de passe. C'est le cas lors de l'enregistrement sur certains sites Internet, lors de l'achat dans des boutiques en ligne, etc.

Le risque existe que ces données soient interceptées à l'aide d'outils d'interception ou d'enregistreurs de frappes.

Le clavier virtuel permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.

Le clavier virtuel ne peut protéger vos données si le site nécessitant la saisie de ces données a été compromis car dans ce cas, les données tombent directement entre les mains des individus mal intentionnés.

Plusieurs programmes-espions peuvent faire des captures d'écran qui se transmettent automatiquement au malfaiteur pour qu'il analyse et qu'il puisse récupérer les données personnelles de l'utilisateur. Le clavier virtuel protège les données personnelles saisies contre l'interception par les captures d'écran.

Le clavier virtuel protège contre l'interception des données personnelles uniquement si les navigateurs Microsoft Internet Explorer et Mozilla Firefox fonctionnent.

➡ Pour utiliser le clavier virtuel, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Clavier virtuel**.
3. Saisissez les données requises en appuyant sur les touches du clavier virtuel. Assurez-vous que les données sont saisies dans le champ requis. Si vous appuyez sur les touches de fonction (**Maj**, **Alt** ou **Ctrl**) du clavier virtuel, le mode de saisie spécial est activé (ainsi, si vous appuyez sur la touche **Maj**, tous les caractères seront saisis en majuscules). Pour annuler un mode spécial, appuyez à nouveau sur la touche de fonction.

DISQUE DE DEPANNAGE

Kaspersky Anti-Virus propose la création d'un disque de dépannage.

Le disque de dépannage est prévu pour le contrôle et la réparation des ordinateurs (compatibles x86) infectés. Il est utilisé lors de tel degré d'infection, quand il n'est pas possible de réparer l'ordinateur par les applications antivirus ou par les utilitaires de réparation (par exemple, Kaspersky AVPTool), lancés sous le système d'exploitation. Avec cela, l'efficacité de réparation est augmentée grâce au fait que les programmes malveillants dans le système ne reçoivent pas d'administration pendant le démarrage du système d'exploitation.

Le disque de dépannage est créé à la base du noyau du système d'exploitation Linux et représente le fichier .iso qui inclut :

- les fichiers de système et de configuration Linux ;
- un ensemble d'utilitaires pour le diagnostic du système d'exploitation ;
- l'ensemble d'utilitaires auxiliaires (le gestionnaire de fichiers, etc.) ;
- les fichiers Kaspersky Rescue Disk ;
- les fichiers contenant les bases antivirus.

Le démarrage de l'ordinateur avec le système d'exploitation endommagé peut être effectué du périphérique CD/DVD-ROM. Pour cela le périphérique correspondant doit être installé sur l'ordinateur.

➡ Afin de créer le disque de dépannage, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Utilitaires+**.
3. Cliquez sur **Disque de dépannage** afin de lancer l'assistant de création de disque.
4. Suivez les consignes de l'Assistant.
5. A l'aide du fichier obtenu à la fin de l'Assistant, créez un CD/DVD de dépannage. Vous pouvez utiliser pour ce faire un des programmes d'enregistrement de CD/DVD tel que Nero par exemple.

VOIR EGALEMENT

Création d'un disque de dépannage	123
Démarrage de l'ordinateur à l'aide du disque de dépannage.....	123

CREATION D'UN DISQUE DE DEPANNAGE

La création du disque de dépannage consiste à générer une image du disque (fichier .iso) à partir des bases antivirus actuelles ainsi que des fichiers de configuration.

L'image du disque de départ, en fonction de laquelle le nouveau fichier est généré, peut être téléchargée du serveur de Kaspersky Lab, ou copiée depuis une source locale.

Le fichier de l'image, généré par l'Assistant, est sauvegardé dans le dossier "*Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP9\Data\Rdisk*" ("*ProgramData\Kaspersky Lab\AVP9\Data\Rdisk*" : pour Microsoft Vista) avec le nom *rescuecd.iso*. Si l'Assistant a découvert le fichier de l'image, créé précédemment, dans le dossier, alors, en cochant la case ☒ **Utiliser l'image existante**, vous pouvez l'utiliser en guise de l'image du disque de départ, et passez tout d'un coup à l'étape 3 : mise à jour de l'image. Si l'Assistant n'a pas découvert le fichier de l'image, alors cette case n'existe pas.

La création du disque de dépannage s'opère à l'aide d'un assistant spécial qui contient une succession de fenêtres (étape) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Pour terminer le travail de l'assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

VOIR EGALEMENT

Disque de dépannage	122
Démarrage de l'ordinateur à l'aide du disque de dépannage.....	123

DEMARRAGE DE L'ORDINATEUR A L'AIDE DU DISQUE DE DEPANNAGE

S'il est impossible de charger le système d'exploitation suite à une attaque de virus, utilisez le disque de dépannage.

Pour charger le système d'exploitation, il vous faut absolument un fichier d'image (.iso) de disque de dépannage. Vous pouvez charger le fichier depuis le serveur de Kaspersky Lab ou actualiser le fichier existant.

Examinons en détails le fonctionnement du disque de dépannage. Les opérations suivantes se déroulent durant le chargement du disque :

1. Identification automatique de la configuration matérielle de l'ordinateur.
2. Recherche de systèmes de fichiers sur les disques durs. Les systèmes de fichiers trouvés sont identifiés par un nom commençant par C.

Les noms attribués aux disques durs et aux disques amovibles peuvent ne pas correspondre à la dénomination dans le système d'exploitation.

Si le système d'exploitation d'ordinateur démarré est en mode de veille, ou son système de fichiers est en mode *unclean*, en conséquence de l'arrêt incorrect du fonctionnement, il vous sera proposé de prendre une décision sur l'assemblage du système de fichiers ou de redémarrer l'ordinateur.

L'assemblage du système de fichiers peut amener à sa panne.

3. Recherche d'un fichier de téléchargement Microsoft Windows *pagefile.sys*. Si ce fichier n'existe pas, la taille de la mémoire virtuelle est limitée par la taille de la mémoire vive.
4. Choix de la langue de la version. Si durant une certaine période de temps, aucune sélection n'a eu lieu, alors la langue anglaise est prise par défaut.
5. Recherche (création) des dossiers pour le placement des bases antivirus, des rapports, de la quarantaine et des fichiers auxiliaires. Les répertoires de l'application de Kaspersky Lab installée sur l'ordinateur infectés sont utilisés par défaut (*ProgramData/Kaspersky Lab/AVP9* – pour Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP9* – pour les versions antérieures de Microsoft Windows). Si les répertoires de l'application sont introuvables, une tentative de création sera réalisée. Si les dossiers n'ont pas été découverts et il n'a pas été possible de les créer, le dossier *kl.files* se crée sur un des disques.
6. La tentative de configurer les connexions de réseau en fonction des données, découvertes dans les fichiers de système de l'ordinateur démarré.
7. Chargement du sous-système graphique et lancement de Kaspersky Rescue Disk.

En mode de restauration, seules la recherche de virus et la mise à jour des bases depuis une source locale sont accessibles, aussi que l'annulation des mises à jour et la consultation des statistiques.

➡ *Pour lancer le système d'exploitation d'un ordinateur infecté, procédez comme suit :*

1. Dans les paramètres BIOS, activez le chargement depuis un CD/DVD (pour obtenir de plus amples informations, consultez la documentation de la carte mère de votre ordinateur).
2. Introduisez le disque contenant l'image du disque de dépannage dans le lecteur d'un ordinateur infecté.
3. Redémarrez l'ordinateur.

Le chargement est alors exécuté conformément à l'algorithme décrit ci-dessus. L'aide de Kaspersky Rescue Disk contient de plus amples informations sur les possibilités du disque de dépannage.

VOIR ÉGALEMENT

Disque de dépannage	122
Création d'un disque de dépannage	123

CONFIGURATION DU NAVIGATEUR

L'Assistant de configuration du navigateur analyse les paramètres de Microsoft Internet Explorer du point de vue de la sécurité car certaines valeurs attribuées par l'utilisateur ou définies par défaut peuvent engendrer des problèmes de sécurité.

L'Assistant vérifie si les mises à jour les plus récentes du navigateur sont installées et si les paramètres de ce dernier constituent des vulnérabilités qui pourraient être utilisées par des individus mal intentionnés dans le but de nuire à l'ordinateur. Voici des exemples d'objets analysés :

- **Cache de fonctionnement de Microsoft Internet Explorer.** Le cache contient des données confidentielles et permet de voir les sites visités par l'utilisateur. Nombreux sont les objets malveillants qui lors du balayage du disque balaient également le cache, ce qui signifie que les individus mal intentionnés peuvent obtenir les adresses de messagerie des utilisateurs. Il est conseillé de nettoyer le cache après l'utilisation du navigateur.
- **Affichage de l'extension pour les fichiers de format connu.** Il est utile pour l'utilisateur de voir l'extension réelle du fichier. De nombreux objets malveillants utilisent des extensions doubles. Dans ce cas, l'utilisateur voit uniquement une partie du nom du fichier sans l'extension réelle. Cette méthode est largement employée par les individus mal intentionnés. Il est conseillé d'activer l'affichage de l'extension pour les fichiers de format connu.

- **Liste des sites de confiance.** Les objets malveillants peuvent être ajoutés à la liste des liens vers des sites créés par des individus mal intentionnés.

Avant de lancer le diagnostic, fermez toutes les fenêtres de Microsoft Internet Explorer.

Une l'étude terminée, l'Assistant analyse les informations recueillies afin d'identifier les problèmes de sécurité dans les paramètres du navigateur qui doivent être réglés sur le champ. Le résultat de l'étude se présente sous la forme d'une liste d'action qu'il convient d'exécuter pour supprimer le problème. Les actions sont groupées en catégorie selon la gravité des problèmes identifiés.

Pour conclure, l'Assistant rédige un rapport qui peut être envoyé à Kaspersky Lab pour analyse.

Il ne faut pas oublier que certaines valeurs des paramètres peuvent entraîner des problèmes d'affichage de certains sites (par exemple, si ces sites utilisent des éléments ActiveX). Vous pouvez résoudre ce problème en ajoutant ces sites à la zone de confiance.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

➡ Pour lancer l'Assistant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Paramètres et réglages du navigateur**.

RESTAURATION APRES INFECTION

L'Assistant de restauration après infection permet de liquider les traces de la présence d'objets malveillants dans le système. Les experts de Kaspersky Lab recommandent de lancer l'Assistant après la réparation de l'ordinateur afin de confirmer que toutes les menaces et les dégâts qu'elles ont causés ont été supprimés. De plus, l'Assistant peut être utilisé si vous pensez que l'ordinateur est infecté.

L'Assistant vérifie si le système a été modifié d'une manière ou d'une autre : blocage de l'accès à l'environnement de réseau, modification des extensions de fichiers de format connu, blocage du panneau d'administration, etc. Ces comportements peuvent être provoqués par divers éléments tels que l'activité de programmes malveillants, par des échecs du système ou par l'utilisation de logiciels d'optimisation du système qui ne fonctionnent pas correctement.

Après l'étude, l'Assistant analyse les informations recueillies afin d'identifier les dégâts dans le système qui requièrent une intervention immédiate. Le résultat de l'étude se présente sous la forme d'une liste d'action qu'il convient d'exécuter pour supprimer la corruption. Les actions sont groupées en catégorie selon la gravité des problèmes identifiés.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

➡ Pour lancer l'Assistant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Restauration du système**.

ASSISTANT DE SUPPRESSION DES TRACES D'ACTIVITE

Lorsque vous utilisez votre ordinateur, vos activités sont enregistrées dans le système. Dans ce contexte, les données suivantes sont enregistrées :

- Historique contenant des informations sur :
 - La visite de sites Internet ;
 - L'exécution de l'application ;
 - Les recherches ;
 - L'ouverture/l'enregistrement de fichiers par diverses applications.
- Les enregistrements dans le journal système de Microsoft Windows.
- Les fichiers temporaires, etc.

Toutes ces sources d'informations sur l'activité de l'utilisateur peuvent contenir des données confidentielles (y compris des mots de passe) que les individus mal intentionnés pourraient analyser. Bien souvent, l'utilisateur ne possède pas les connaissances suffisantes pour empêcher ce genre de vol d'informations de valeur.

Kaspersky Anti-Virus propose un assistant de **Suppression des traces d'activité**. Cet Assistant recherche les traces d'activité de l'utilisateur dans le système ainsi que les paramètres du système d'exploitation qui permettent de récolter des informations sur cette activité.

Le système ne cesse d'accumuler des informations sur l'activité de l'utilisateur. L'exécution du moindre fichier ou l'ouverture de n'importe quel document est enregistrée dans l'historique et le journal de Microsoft Windows enregistre une multitude d'événements qui surviennent dans le système. Ceci veut dire qu'une nouvelle exécution de l'assistant de **Suppression des traces d'activité** peut découvrir des traces supprimées lors de l'exécution antérieure de l'Assistant. Certains fichiers, par exemple le fichier de rapport de Microsoft Windows, peuvent être utilisés par le système au moment où ils sont supprimés par l'Assistant. Afin de pouvoir supprimer les fichiers, l'Assistant propose de redémarrer le système. Toutefois, ces fichiers peuvent être recréés lors du redémarrage, ce qui signifie qu'ils seront à nouveau découverts en tant que trace d'activité.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

➡ *Pour lancer l'Assistant, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Suppression des traces d'activité**.

RAPPORTS

Le fonctionnement de chaque composant de Kaspersky Anti-Virus et l'exécution de chaque tâche de recherche de virus et de mise à jour sont consignés dans le rapport.

Lors de l'utilisation des rapports, vous pouvez réaliser les opérations suivantes :

- sélectionner le composant / la tâche (cf. page [127](#)) au sujet duquel vous souhaitez consulter le rapport ;
- administrer les groupes de données (cf. page [128](#)) et les présenter à l'écran (cf. page [130](#)) ;
- composer l'horaire (cf. page [129](#)) selon lequel Kaspersky Anti-Virus vous rappellera que le rapport est prêt ;
- sélectionner le type d'événement (cf. page [129](#)) pour lequel il faut générer un rapport ;
- choisir la forme sous laquelle les statistiques seront présentées : tableau ou graphique (cf. page [131](#)) ;
- enregistrer le rapport dans un fichier (cf. page [131](#)) ;
- définir des conditions de filtrage complexes (cf. page [131](#)) ;
- organiser la recherche d'événements (cf. page [132](#)) survenus dans le système et traités par l'application.

DANS CETTE SECTION

Sélection du composant ou de la tâche pour la composition du rapport.....	127
Administration des groupes d'informations dans le rapport	128
Notification sur la disponibilité du rapport.....	129
Sélection du type d'événement.....	129
Présentation des données à l'écran	130
Présentation des données statistiques dans un tableau ou dans un graphique.....	131
Enregistrement du rapport dans un fichier.....	131
Utilisation du filtrage complexe	131
Recherche d'événements.....	132

SELECTION DU COMPOSANT OU DE LA TACHE POUR LA COMPOSITION DU RAPPORT

Vous pouvez obtenir des informations sur les événements survenus pendant le fonctionnement de chaque composant de Kaspersky Anti-Virus ou lors de l'exécution de tâches (par exemple, Antivirus Fichiers, mise à jour, etc.)

➤ Pour obtenir un rapport sur un composant ou une tâche quelconque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la liste déroulante située à gauche dans la fenêtre qui s'ouvre, choisissez le composant ou la tâche pour lequel vous souhaitez générer un rapport. Si vous choisissez l'option **Protection**, le rapport sera produit pour tous les composants de la protection.

ADMINISTRATION DES GROUPES D'INFORMATIONS DANS LE RAPPORT

Vous pouvez administrer le regroupement des données présentées dans le rapport ; dans ce cas, les informations seront regroupées selon divers critères. La sélection des critères varie en fonction des composants et des tâches. Vous avez le choix entre :

- **Sans regroupement.** Tous les événements seront présentés.
- **Regroupement par tâche.** Les données seront regroupées en fonction des tâches exécutées par les composants de Kaspersky Anti-Virus.
- **Regroupement par application.** Les données seront regroupées en fonction des applications actives dans le système et traitées par Kaspersky Anti-Virus.
- **Regroupement selon le résultat.** Les données seront regroupées en fonction des résultats de l'analyse ou du traitement de l'objet.

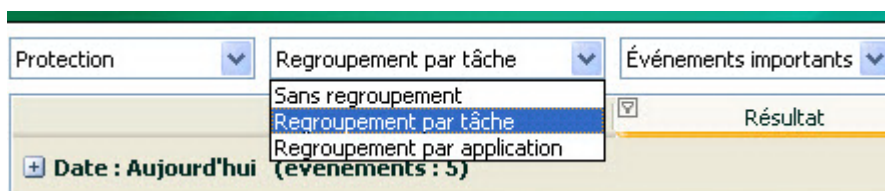


Illustration 13 : Critères de regroupement des informations dans le rapport

Afin d'obtenir rapidement les informations requises et de réduire la taille des groupes, il est possible de lancer une recherche (cf. section "Recherche d'événements" à la page [132](#)) sur la base de mot clé. Vous pouvez définir également des critères de recherche.

➤ Pour réaliser le regroupement selon un critère quelconque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, sélectionnez le critère de regroupement dans le menu déroulant.

NOTIFICATION SUR LA DISPONIBILITE DU RAPPORT

Vous pouvez programmer la fréquence selon laquelle Kaspersky Anti-Virus vous rappellera la disponibilité des rapports.

➤ *Pour programmer l'envoi de notifications, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cochez la case ☒ **Rappeler le rapport**. Cliquez sur le lien avec l'heure définie.
3. Dans la fenêtre **Rapport: programmation** qui s'ouvre, programmez l'envoi.

SELECTION DU TYPE D'EVENEMENT

La liste complète de l'ensemble des événements survenus durant le fonctionnement du composant de la protection, de l'exécution de l'analyse ou de la mise à jour des bases de l'application figure dans le rapport. Vous pouvez sélectionner les types d'événement qui seront repris dans le rapport.

Les événements peuvent appartenir aux catégories suivantes :

- *Événements critiques.* Événements critiques qui indiquent un problème dans le fonctionnement de Kaspersky Anti-Virus ou une vulnérabilité dans la protection de l'ordinateur. Il s'agit par exemple de la découverte d'un virus ou d'un échec de fonctionnement.
- *Événements importants.* Événements auxquels il faut absolument prêter attention car ils indiquent une situation dans le fonctionnement du logiciel qui nécessite une intervention, par exemple l'événement **interrompu**.

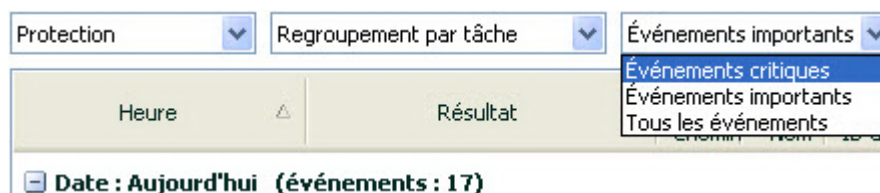


Illustration 14 : Sélection du type d'événement

Lors de la sélection du point **Tous les événements**, tous les événements seront reflétés dans le rapport, mais uniquement si dans la section **Rapports et Stockages**, groupe **Rapports** les cases sont cochées (cf. section "Ajout d'enregistrements relatifs aux événements dans le rapport" à la page 115) qui permettent de donner les informations dans le rapport d'écriture sur les événements non-critiques, de même du système de fichiers et du registre. Si les cases sont décochées, à côté de la liste avec le choix des types d'événements le lien **Désactivé** et un avertissement sont reflétés. Utilisez ce lien pour passer à la fenêtre de configuration des rapports et cochez les cases qu'il faut.

➤ *Pour sélectionner le type d'événement pour lequel il faut composer un rapport, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, sélectionnez le type d'événement dans le menu. S'il faut générer un rapport pour l'ensemble des événements, sélectionnez l'option **Tous les événements**.

PRESENTATION DES DONNEES A L'ECRAN

Les événements repris dans le rapport sont présentés sous la forme d'un tableau. Vous pouvez sélectionner les informations en définissant des conditions de restriction. Pour ce faire, cliquez avec le bouton gauche de la souris à gauche du titre de la colonne du tableau pour laquelle vous souhaitez introduire une restriction. La liste déroulante contient les restrictions, par exemple, **Hier** pour la colonne **Heure**, **Courrier électronique** pour la colonne **Objet**, etc. Faites votre choix. Choisissez l'option requise ; la sélection des données s'opèrera sur la base de la restriction définie. Si vous devez consulter l'ensemble des données, sélectionnez l'option **Tous** dans la liste des restrictions.

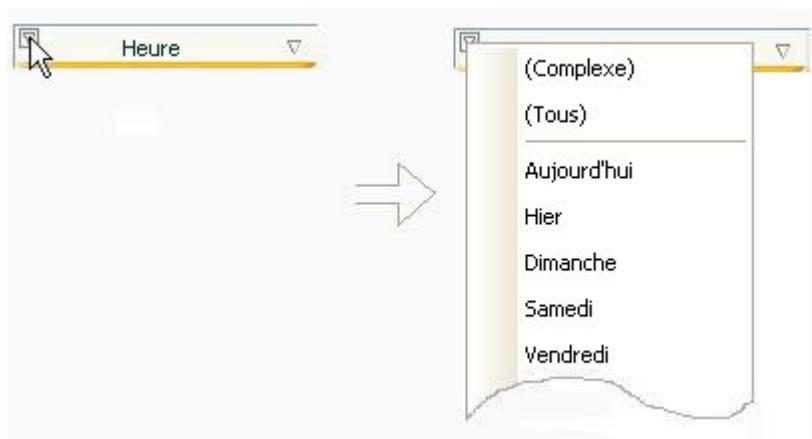


Illustration 15 : Définition d'une restriction

De plus, vous pouvez définir les paramètres de recherche complexe sous la forme d'une plage dans le cadre de laquelle il faudra sélectionner les données sur les événements survenus. Pour ce faire, dans la liste déroulante des restrictions, choisissez l'option **Complexe**. Dans la fenêtre qui s'ouvre définissez l'intervalle requis (cf. section "Utilisation du filtrage complexe" à la page [131](#)).

Pour simplifier l'utilisation de l'onglet, il existe un menu contextuel qui permet d'accéder rapidement à n'importe quelle caractéristique permettant de regrouper et de sélectionner les événements.

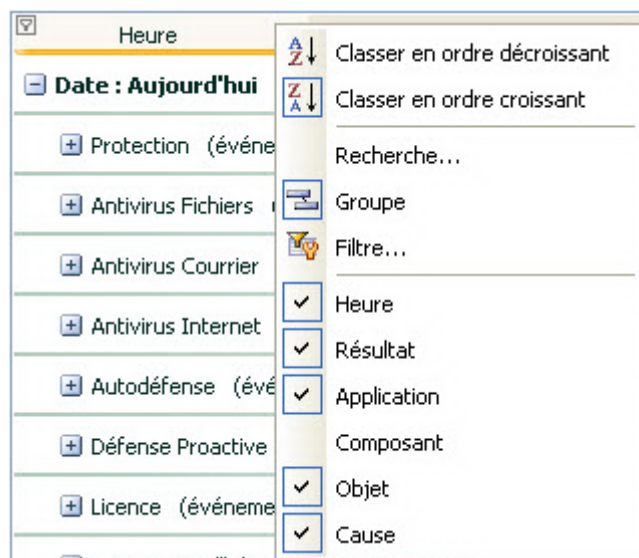


Illustration 16: Menu contextuel

► Pour définir la condition de restriction, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.

3. Dans la fenêtre qui s'ouvre, cliquez avec le bouton gauche de la souris à gauche du titre de la colonne dans laquelle vous souhaitez introduire une restriction. Choisissez la restriction voulue dans la liste déroulante. Lors de la sélection du point **Complexe**, vous pouvez définir les conditions complexes du filtrage (cf. section "Utilisation du filtrage complexe" à la page [131](#)).

➤ *Pour afficher / dissimuler les colonnes du tableau, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, cliquez avec le bouton droit de la souris à droite du titre de n'importe quelle colonne du tableau. Pour dissimuler certaines colonnes du tableau, décochez la case en regard du nom correspondant dans le menu contextuel.

PRESENTATION DES DONNEES STATISTIQUES DANS UN TABLEAU OU DANS UN GRAPHIQUE

La partie inférieure de la fenêtre des rapports reprend les statistiques de fonctionnement du composant ou de la tâche de Kaspersky Anti-Virus sélectionné. Vous pouvez consulter les statistiques et choisir le format de présentation (graphique (pour les composants) ou tableau). La sélection de la représentation s'effectue à l'aide des boutons  et  en haut de la fenêtre. Les statistiques présentées concernent la journée en cours ou toute la période pendant laquelle l'application a fonctionné sur l'ordinateur.

➤ *Pour sélectionner le type de représentation des statistiques, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, sélectionnez le composant de l'application dont vous souhaitez consulter les statistiques et utilisez les boutons  et  dans la partie supérieure de la fenêtre.

ENREGISTREMENT DU RAPPORT DANS UN FICHIER

Le rapport obtenu peut être enregistré dans un fichier.

➤ *Pour enregistrer le rapport dans un fichier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, rédigez le rapport requis, puis cliquez sur le bouton **Enregistrer**.
4. Dans la fenêtre qui s'ouvre, désignez le répertoire dans lequel il faut enregistrer le fichier du rapport et saisissez le nom du fichier.

UTILISATION DU FILTRAGE COMPLEXE

La fenêtre **Filtre complexe** (cf. ill. ci-après) permet de définir les paramètres du filtrage complexe des données. Vous pouvez définir la plage de recherche des données pour n'importe quelle colonne du tableau. Nous allons étudier les principes de fonctionnement à l'aide de la colonne **Heure**.

La sélection des données à l'aide d'un filtre repose sur les opérations logiques de conjonctions (ET logique) et de disjonction (OU logique) qui permettent d'administrer la sélection des données.

Dans les champs situés dans la partie droite de la fenêtre, définissez les limites de la sélection (dans ce cas-ci, il s'agit de l'heure). Pour définir l'heure, vous pouvez utiliser les touches fléchées du clavier. Dans la partie gauche, la liste déroulante **Condition** vous permet de sélectionner la condition de sélection des événements, par exemple, **supérieur**, c.-à-d. supérieur à la limite définie dans le champ à droite.

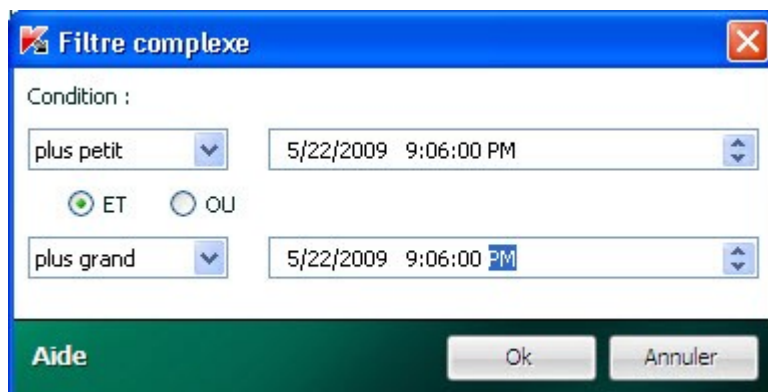


Illustration 17 : Définition des conditions de filtrage complexe

Si vous souhaitez que la sélection des données vérifie les deux conditions définies, sélectionnez **ET**. Si une condition minimum suffit, sélectionnez **OU**.

Pour toute une série de colonnes, les limites de la plage de recherche ne sont ni des chiffres, ni des heures, mais un mot (par exemple, résultat de l'analyse **OK** pour la colonne **Résultat**). Dans ce cas, le mot, défini en tant que limite, est comparé aux autres mots-valeurs pour la colonne sélectionnée par ordre alphabétique.

➤ Pour définir les conditions complexes du filtrage, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, cliquez avec le bouton gauche de la souris à gauche du titre de la colonne pour laquelle vous souhaitez définir les conditions de filtrage complexe. Sélectionnez le point **Complexe** dans le menu déroulant. Vous pouvez également choisir l'option **Filtre** dans le menu contextuel (cf. section "Présentation des données à l'écran" à la page [130](#)) accessible d'un clic avec le bouton droit de la souris sur la colonne souhaitée.
4. Dans la fenêtre **Filtre complexe** définissez les conditions nécessaires du filtrage.

RECHERCHE D'EVENEMENTS

Cette fenêtre (cf. ill. ci-après) permet de rechercher les événements survenus dans le système et traités par Kaspersky Anti-Virus.

Examinons les principes de fonctionnement :

- Le champ **Ligne** est prévu pour la saisie du mot clé (par exemple, explorer). Pour lancer la recherche, cliquez sur le bouton **Recherche avancée**. La recherche des données peut prendre un certain temps. A la fin de la recherche, vous pourrez voir les événements qui correspondent au mot clé utilisé. Si vous cliquez sur le bouton **Marquer tout**, toutes les données qui satisfont le mot clé saisi seront mises en évidence.

- Le champ **Colonne** permet de sélectionner la colonne du tableau dans laquelle la recherche du mot clé aura lieu. Ce choix permet de réduire le temps consacré à la recherche (si, bien évidemment, la valeur **Tous** n'a pas été sélectionnée).



Illustration 18 : Recherche d'événements

Si vous souhaitez que la recherche tiennent compte de la case pour le mot clé, cochez la case ☒ **Respecter la case**. La case ☒ **Uniquement les mots entiers** permet de limiter les résultats de la recherche et d'afficher uniquement ceux correspondant aux mots entiers définis du mot clé.

➡ Pour utiliser la recherche d'événements, procédez comme suit :

- Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
- Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
- Dans la fenêtre qui s'ouvre, cliquez avec le bouton droit de la souris à droite du titre de n'importe quelle colonne du tableau. Dans le menu qui s'ouvre, sélectionnez le point **Recherche**.
- Dans la fenêtre ouverte **Recherche** définissez le critère de recherche.

NOTIFICATIONS

Lorsqu'un événement se produit pendant l'utilisation de Kaspersky Anti-Virus, vous verrez apparaître un message spécial. En fonction de la gravité de l'événement pour la sécurité de l'ordinateur, les notifications peuvent appartenir aux catégories suivantes :

- **Alertes.** Un événement critique s'est produit, par exemple un objet malveillant ou une activité dangereuse a été découvert dans le système. Il faut immédiatement décider de la suite des événements. La fenêtre de ce genre de notification est rouge.
- **Attention.** Un événement qui présente un risque potentiel s'est produit, par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système. Il est indispensable de décider, selon vous, à quel point cette action est dangereuse. La fenêtre de ce genre de notification est orange.
- **Informations.** Ce message vous signale un événement qui n'est pas critique. La fenêtre de ce genre de notification est verte.

La fenêtre de notification contient quatre parties :

1. *Titre de la fenêtre.* Le titre de la fenêtre fournit une brève description de l'événement, par exemple : demande de privilèges, activité suspecte, nouveau réseau, alerte, virus, etc.
2. *Description de l'événement.* Le groupe de description de l'événement fournit des détails sur la cause de la notification : nom de l'application à l'origine de l'événement, nom de la menace détectée, paramètres de la connexion de réseau détectée, etc.
3. *Zone de sélection de l'action.* Ce groupe vous propose de choisir entre plusieurs actions possibles pour ce type d'événement. Les options proposées dépendent du type d'événement, par exemple : **Réparer**, **Supprimer**, **Ignorer** en cas de découverte d'un virus, **Autoriser**, **Interdire** lorsque l'application demande des privilèges pour exécuter des actions présentant un danger potentiel. L'action recommandée par les experts de Kaspersky Lab est écrite en caractères gras.

Lors de la sélection de l'action **Autoriser** ou **Interdire**, une fenêtre s'ouvre, où vous pouvez sélectionner le *mode d'utilisation de l'action*. Pour l'action **Autoriser** vous pouvez sélectionner un des modes suivants :

- **Autoriser toujours.** Cochez cette case pour résoudre l'activité découverte du programme par les changements dans la règle d'accès du programme vers les ressources du système.
- **Autoriser maintenant.** Cochez cette case pour appliquer l'action sélectionnée à tous les événements identiques découverts pendant la session de fonctionnement de l'application. La session de fonctionnement d'une application désigne la période entre le moment où elle a été lancée et le moment où elle est arrêtée ou redémarrée.
- **Rendre fiable.** Cochez cette case pour transmettre l'application dans le groupe **De confiance**.

Pour l'action **Interdire** vous pouvez sélectionner un des modes suivants :

- **Interdire toujours.** Cochez cette case pour interdire l'activité découverte du programme par les changements dans la règle d'accès du programme vers les ressources du système.
- **Interdire maintenant.** Cochez cette case pour appliquer l'action sélectionnée à tous les événements identiques découverts pendant la session de fonctionnement de l'application. La session de fonctionnement d'une application désigne la période entre le moment où elle a été lancée et le moment où elle est arrêtée ou redémarrée.
- **Quitter.** Cochez cette case pour interrompre le fonctionnement du programme.

4. *Zone de sélection de l'action complémentaire.* Ce groupe permet de sélectionner l'action complémentaire :

- **Ajouter aux exclusions.** Si vous êtes persuadé que l'objet découvert ne présente aucun danger, vous pouvez l'ajouter à la zone de confiance afin d'éviter un nouveau déclenchement de l'application lors d'une nouvelle manipulation de cet objet.
- **Appliquer à tous les objets.** Cochez cette case pour que l'action soit appliquée à tous les objets du même état dans des situations analogues.

DANS CETTE SECTION

Un objet suspect a été détecté	135
La réparation de l'objet est impossible	136
Une procédure spéciale de réparation est requise.....	136
Un objet dangereux a été découvert dans le trafic.....	137
Un objet suspect a été détecté	137
Une activité dangereuse a été découverte dans le système.....	138
Un processus caché a été découvert	139
Une tentative d'accès à la base de registres système a été découverte	139
Une tentative de phishing a été découverte.....	140
Un lien suspect a été découvert.....	140
Découverte d'un certificat incorrect.....	140

UN OBJET SUSPECT A ETE DETECTE

Lorsque l'Antivirus Fichiers, l'Antivirus Courrier ou une tâche d'analyse découvre un objet malveillant, un message spécial apparaît.

Il indique :

- Le type de menace (par exemple : *virus*, *cheval de Troie*) et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.
- Le nom complet de l'objet malveillant et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Réparer** : tentative de réparation de l'objet malveillant. Une copie de sauvegarde est créée avant la suppression au cas où il faudrait restaurer l'objet ou le scénario de l'infection.
- **Effacer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.
- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☒ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusqu'à sa fin.

LA REPARATION DE L'OBJET EST IMPOSSIBLE

Dans certains cas, il est impossible de réparer l'objet malveillant. Par exemple, si l'objet est corrompu à un tel point qu'il est impossible d'en supprimer le code malveillant ou de le restaurer. De plus il existe certains types d'objets malicieux comme les chevaux de Troie qui ne peuvent pas être réparés.

Dans ce cas, un message spécial contenant les informations suivantes s'affiche :

- Le type de menace (par exemple : *virus, cheval de Troie*) et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.
- Le nom complet de l'objet malveillant et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Effacer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.
- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action, sauf consigner les informations à son sujet dans le rapport.

Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☒ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche d'analyse antivirus depuis son lancement jusqu'à sa fin.

UNE PROCEDURE SPECIALE DE REPARATION EST REQUISE

Suite à la découverte d'une menace active en ce moment dans le système (par exemple, un processus malveillant dans la mémoire vive ou dans les objets de démarrage), un message vous invitant à lancer la procédure de réparation élargie s'affiche.

Les experts de Kaspersky Lab recommandent vivement d'accepter de lancer cette procédure de réparation. Pour ce faire, cliquez sur le bouton **OK**. Toutefois, n'oubliez pas que l'ordinateur sera redémarré à la fin de la procédure et par conséquent, il est conseillé d'enregistrer tous les travaux en cours et de quitter toutes les applications avant de lancer la procédure.

Lors de la procédure de réparation, il est interdit de lancer les clients de messagerie ou de modifier les bases de registres système du système d'exploitation. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète.

UN OBJET DANGEREUX A ETE DECOUVERT DANS LE TRAFIC

Lorsque l'Antivirus Internet découvre un objet dangereux dans le trafic, un message spécial s'affiche.

Celui-ci contient :

- Le type de menace (par exemple : *modification d'un virus*) et le nom de l'objet dangereux tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte.
- Le nom complet de l'objet dangereux et le chemin vers la ressource Internet.

Vous aurez le choix entre les actions suivantes :

- **Autoriser** : continue à télécharger l'objet.
- **Interdire** : bloque le téléchargement de l'objet depuis le site Internet.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☒ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusqu'à sa fin.

UN OBJET SUSPECT A ETE DETECTE

Lorsque l'Antivirus Fichiers, l'Antivirus Courrier ou la recherche d'éventuels virus découvre un objet qui contient le code d'un virus inconnu ou le code modifié d'un virus connu, un message spécial s'affiche.

Il indique :

- Le type de menace (par exemple : *virus, cheval de Troie*) et le nom de l'objet tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.
- Le nom complet de l'objet et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Quarantaine** : place l'objet en quarantaine. Dans ce cas, l'objet est déplacé et non pas copié : l'objet est supprimé du disque ou du message et il est enregistré dans le répertoire de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement OK. Cela se passe uniquement si l'analyse a été réalisée (dans les trois jours maximum) après la mise en quarantaine du fichier.

- **Supprimer** : supprime l'objet. Avant la suppression une copie de sauvegarde de l'objet est créée au cas où il faudra par la suite le restaurer ou reproduire le scénario de l'infection.

- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

Vous pourrez revenir au traitement des objets ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☒ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusqu'à sa fin.

Si vous êtes convaincu que l'objet découvert n'est pas malveillant, il est conseillé de l'ajouter à la zone de confiance pour éviter tout nouveau déclenchement de l'activation lors d'une prochaine manipulation de cet objet.

UNE ACTIVITE DANGEREUSE A ETE DECOUVERTE DANS LE SYSTEME

Lorsque la Protection proactive découvre une activité dangereuse en provenance d'une application quelconque du système, un message spécial apparaît avec les informations suivantes :

- Nom de la menace, tel qu'il figure dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte.
- Le nom complet du fichier du processus à l'origine de l'activité dangereuse et son chemin d'accès.
- Sélection des actions possibles :
 - **Quarantaine** : arrêter le processus et mettre son fichier exécutable en quarantaine. Un objet qui est mis en quarantaine est déplacé et non pas copié. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement OK. Cela se passe uniquement si l'analyse a été réalisée (dans les trois jours maximum) après la mise en quarantaine du fichier.

- **Terminer** : terminer le processus.
- **Autoriser** : autoriser l'exécution du processus.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☒ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusqu'à sa fin.

Si vous êtes convaincu que l'application découverte ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky Anti-Virus.

UN PROCESSUS CACHE A ETE DECOUVERT

Lorsque la Protection proactive découvre un processus caché dans le système, un message spécial s'affiche et fournit les informations suivantes :

- Nom de la menace, tel qu'il figure dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte.
- Le nom complet du processus caché et son chemin d'accès.
- Sélection des actions possibles :
 - **Quarantaine** : place le fichier exécutable du processus en quarantaine. Un objet qui est mis en quarantaine est déplacé et non pas copié. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement OK. Cela se produira uniquement si l'analyse a eu lieu un certain temps (au moins trois jours) après la mise du fichier en quarantaine.

- **Terminer** : terminer le processus.
- **Autoriser** : autoriser l'exécution du processus.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☒ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusqu'à sa fin.

Si vous êtes convaincu que l'application découverte ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky Anti-Virus.

UNE TENTATIVE D'ACCES A LA BASE DE REGISTRE SYSTEME A ETE DECOUVERTE

Lorsque la Défense Proactive découvre une tentative d'accès aux clés de la base de registre système, un message spécial s'affiche et fournit les informations suivantes :

- La clé du registre exposée à la tentative d'accès.
- Le nom complet du fichier du processus à l'origine de la tentative d'accès à la clé du registre et son chemin d'accès.
- Sélection des actions possibles :
 - **Autoriser** : autorise une fois l'exécution de l'action dangereuse ;
 - **Interdire** : interdit une fois l'exécution de l'action dangereuse.

Pour que l'action que vous avez sélectionnée soit exécutée automatiquement chaque fois qu'une telle activité sera lancée sur l'ordinateur, cochez la case ☒ **Créer une règle**.

Si vous estimez qu'aucune des actions lancées par l'application qui a tenté d'accéder à la base de registres système n'est dangereuse, vous pouvez ajouter l'application à la liste des applications de confiance.

UNE TENTATIVE DE PHISHING A ETE DECOUVERTE

Lorsque Kaspersky Anti-Virus découvre une tentative d'ouverture d'un site de phishing, un message spécial s'affiche.

Celui-ci contient :

- Le nom de la menace, *attaque de phishing*, sous la forme de lien qui vous renvoie à la description détaillée de la menace dans l'Encyclopédie des virus de Kaspersky Lab.
- L'URL du site de phishing.
- Sélection des actions possibles :
 - **Autoriser** : continue à télécharger le site de phishing.
 - **Interdire** : bloque le téléchargement du site de phishing.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☒ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusqu'à sa fin.

UN LIEN SUSPECT A ETE DECOUVERT

Lorsque Kaspersky Anti-Virus découvre une tentative d'ouverture d'un site Web dont l'adresse figure dans la liste des URL suspectes, il affiche un message spécial.

Celui-ci contient :

- URL du site
- Sélection des actions possibles :
 - **Autoriser** : poursuit le chargement du site Web.
 - **Interdire** : bloque le chargement du site Web.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☒ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusqu'à sa fin.

DECOUVERTE D'UN CERTIFICAT INCORRECT

L'analyse de la sécurité de connexion par le protocole SSL aura lieu à l'aide du certificat installé. En cas de tentative de connexion avec le serveur avec un certificat incorrect (par exemple, dans le cas de substitution par les malfaiteurs), un message spécial s'affiche.

L'information sur les causes possibles d'erreur, ainsi que le port et l'adresse à distance s'affichent dans la notification. Vous serez invité à décider de la nécessité d'établir la connexion en cas d'utilisation d'un certificat non valide.

- **Accepter le certificat** : poursuivre la connexion à une ressource en ligne ;
- **Rejeter le certificat** : rompre la connexion à une ressource en ligne ;
- **Consulter le certificat** : profiter de la possibilité de consulter l'information sur le certificat.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE KASPERSKY ANTI-VIRUS

Une fois que Kaspersky Anti-Virus a été installé et configuré, vous pouvez vérifier si la configuration est correcte à l'aide d'un virus d'essai et de ses modifications. La vérification doit être réalisée séparément pour chaque composant de la protection/protocole.

DANS CETTE SECTION

Virus d'essai EICAR et ses modifications.....	142
Test de la protection du trafic HTTP.....	143
Test de la protection du trafic SMTP.....	144
Vérification de l'exactitude de la configuration d'Antivirus Fichiers.....	144
Vérification de l'exactitude de la configuration de la tâche d'analyse antivirus.....	145

VIRUS D'ESSAI EICAR ET SES MODIFICATIONS

Ce "virus" d'essai a été développé spécialement par l'organisation  (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus.

Le virus d'essai N'EST PAS UN VIRUS et il ne contient pas de code qui pourrait nuire à votre ordinateur. Toutefois, la majorité des logiciels antivirus le considère comme un virus.

N'utilisez jamais d'authentiques virus pour vérifier le fonctionnement de votre antivirus !

Vous pouvez télécharger le "virus" d'essai depuis le site officiel de l'organisation **EICAR** :
http://www.eicar.org/anti_virus_test_file.htm.

Avant de lancer le téléchargement, il faut absolument désactiver la protection antivirus car le fichier *anti_virus_test_file.htm* sera identifié et traité par l'application comme un objet infecté transmis par le protocole HTTP. N'oubliez pas de réactiver la protection antivirus dès que le téléchargement du virus d'essai sera terminé.

L'application identifie le fichier téléchargé depuis le site de la société **EICAR** comme un objet infecté par un virus **qui ne peut être neutralisé** et exécute l'action définie pour ce genre d'objet.

Vous pouvez également utiliser une modification du virus d'essai standard afin de vérifier le bon fonctionnement de l'application. Pour ce faire, il faut modifier le contenu du virus standard en ajoutant un des préfixes présentés dans le tableau ci-après. Pour créer une modification du virus d'essai, vous pouvez utiliser n'importe quel éditeur de fichier texte ou éditeur hypertexte tel que le **Bloc-Notes de Microsoft** ou **UltraEdit32**, etc.

Vous pouvez vérifier le bon fonctionnement de votre logiciel antivirus à l'aide d'une modification du virus EICAR uniquement si vous possédez des bases antivirus dont la date de publication est postérieure au 24 octobre 2003 (mise à jour cumulée, octobre 2003).

La première colonne du tableau contient les préfixes qu'il faut ajouter en tête de la ligne du virus d'essai traditionnel. La deuxième colonne reprend toutes les valeurs possibles de l'état attribué par l'antivirus à la fin de l'analyse. La troisième colonne contient les informations relatives au traitement que réservera l'application aux objets de l'état indiqué. N'oubliez pas que les actions à réaliser sur les objets sont définies par les paramètres de l'application.

Après avoir ajouté le préfixe au virus d'essai, enregistrez le fichier, par exemple sous le nom : *eicar_dele.com*. Nommez tous les virus modifiés selon le même principe.

Table 1. Modifications du virus d'essai

Préfixe	Etat de l'objet	Informations relatives au traitement de l'objet
Pas de préfixe, "virus" d'essai standard.	Infecté. L'objet contient le code d'un virus connu. Réparation impossible.	L'application identifie l'objet en tant que virus qui ne peut être réparé. Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée.
CORR–	Corrompu.	L'application a pu accéder à l'objet mais n'a pas pu l'analyser car l'objet est corrompu (par exemple, sa structure est endommagée ou le format du fichier est invalide) Les informations relatives au traitement de l'objet figure dans le rapport sur le fonctionnement de l'application.
WARN–	Suspect. L'objet contient le code d'un virus inconnu. Réparation impossible.	L'analyseur heuristique attribue l'état suspect à l'objet. Au moment de la découverte, les bases de l'antivirus ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet.
SUSP–	Suspect. L'objet contient le code modifié d'un virus connu. Réparation impossible.	L'application a découvert une équivalence partielle entre un extrait du code de l'objet et un extrait du code d'un virus connu. Au moment de la découverte, les bases de l'antivirus ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet.
ERRO–	Erreur d'analyse.	Une erreur s'est produite lors de l'analyse de l'objet. L'application ne peut accéder à l'objet car l'intégrité de celui-ci a été violée (par exemple : il n'y a pas de fin à une archive multivolume) ou il n'y a pas de lien vers l'objet (lorsque l'objet se trouve sur une ressource de réseau). Les informations relatives au traitement de l'objet figure dans le rapport sur le fonctionnement de l'application.
CURE–	Infecté. L'objet contient le code d'un virus connu. Réparable.	L'objet contient un virus qui peut être réparé. L'application répare l'objet et le texte du corps du « virus » est remplacé par CURE Vous serez averti de la découverte d'un tel objet.
DELE–	Infecté. L'objet contient le code d'un virus connu. Réparation impossible.	L'application identifie l'objet en tant que virus qui ne peut être réparé. Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée. Vous serez averti de la découverte d'un tel objet.

TEST DE LA PROTECTION DU TRAFIC HTTP

► Pour vérifier l'identification de virus dans le flux de données transmises par le protocole HTTP :

essayez de télécharger le " virus " d'essai depuis le site officiel de l'organisation **EICAR**:
http://www.eicar.org/anti_virus_test_file.htm.

Lors d'une tentative de téléchargement du virus d'essai, Kaspersky Anti-Virus découvre l'objet, l'identifie comme étant infecté et ne pouvant être réparé puis exécute l'action définie dans les paramètres d'analyse du trafic HTTP pour ce type d'objet. Par défaut, la connexion avec le site est coupée à la moindre tentative de téléchargement du virus d'essai et un message indiquera dans le navigateur que l'objet en question est infecté par le virus EICAR-Test-File.

TEST DE LA PROTECTION DU TRAFIC SMTP

Pour vérifier l'identification des virus dans le flux de données transmises via le protocole SMTP, vous pouvez utiliser le système de messagerie qui exploite ce protocole pour le transfert des données.

Il est conseillé de vérifier le fonctionnement d'Antivirus pour le courrier sortant aussi bien sur le corps des messages que les pièces jointes. Pour vérifier la découverte de virus dans le corps des messages, placer le texte du virus d'essai standard ou d'une de ses modifications dans le corps du message.

➤ *Pour ce faire, exécutez les actions suivantes :*

1. Composez le message au format **Texte normal** à l'aide du client de messagerie installé sur l'ordinateur.

Les messages contenant le virus d'essai dans le corps et rédigés au format RTF et HTML ne seront pas analysés !

2. Placez le texte du virus d'essai standard ou modifié au début du message ou joignez un fichier contenant le test d'essai.
3. Envoyez ce message à l'adresse de l'administrateur.

L'application découvre l'objet, l'identifie en tant qu'objet infecté et bloque l'envoi du message.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE L'ANTIVIRUS FICHIERS

➤ *Pour vérifier l'exactitude de la configuration de l'Antivirus Fichiers, procédez comme suit :*

1. Créez un répertoire sur le disque, copiez-y le virus d'essai récupéré sur le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créé.
2. Autorisez la consignation de tous les événements afin que le rapport reprenne les données sur les objets corrompus ou les objets qui n'ont pas été analysés suite à un échec.
3. Exécutez le fichier du virus d'essai ou une de ses modifications.

L'Antivirus Fichiers intercepte la requête adressée au fichier, la vérifie et exécute l'action définie dans les paramètres. En sélectionnant diverses actions à réaliser sur les objets infectés, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Les informations complètes sur les résultats du fonctionnement de l'Antivirus Fichiers sont consultables dans le rapport sur l'utilisation du composant.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE LA TACHE D'ANALYSE ANTIVIRUS

➤ Pour vérifier l'exactitude de la configuration de la tâche d'analyse, procédez comme suit :

1. Créez un répertoire sur le disque, copiez-y le virus d'essai récupéré sur le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créé.
2. Créez une nouvelle tâche d'analyse antivirus et en guise d'objet à analyser sélectionnez le dossier, contenant la sélection de virus d'essai.
3. Autorisez la consignation de tous les événements dans le rapport afin de conserver les données relatives aux objets corrompus ou aux objets qui n'ont pas été analysés suite à l'échec.
4. Lancez la tâche d'analyse antivirus.

Lors de l'analyse, les actions définies dans les paramètres de la tâche seront exécutées au fur et à mesure que des objets suspects ou infectés sont découverts. En sélectionnant diverses actions à réaliser sur les objets infectés, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Toutes les informations relatives aux résultats de l'exécution de la tâche d'analyse sont consultables dans le rapport de fonctionnement du composant.

UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Anti-Virus à l'aide de la ligne de commande. Ce mode vous permet d'exécuter les opérations suivantes :

- lancement et arrêt des composants de l'application ;
- lancement et arrêt de l'exécution des tâches d'analyse antivirus ;
- obtention d'informations relatives à l'état actuel des composants et aux tâches et à leur statistiques;
- analyse des objets sélectionnés ;
- mise à jour des signatures des menaces et des modules de l'application ;
- appel de l'aide relative à la syntaxe de la ligne de commande ;
- appel de l'aide relative à la syntaxe de la ligne de commande ;

Syntaxe de la ligne de commande :

```
avp.com <instruction> [paramètres]
```

La requête adressée à l'application via la ligne de commande doit être réalisée depuis le répertoire d'installation du logiciel ou en indiquant le chemin d'accès complet à avp.com.

Les instructions suivantes sont prévues :

ACTIVATE	activation de Kaspersky Anti-Virus via Internet à l'aide du code d'activation
ADDKEY	activation du programme à l'aide du fichier de la clé de licence (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
START	lancement du composant ou de la tâche
STOP	arrêt du composant ou de la tâche (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky Anti-Virus)
STATUS	affichage de l'état actuel du composant ou de la tâche
STATISTICS	affichage des statistiques du composant ou de la tâche
HELP	aide sur la syntaxe de la commande ou la liste des commandes.
SCAN	analyse antivirus des objets
UPDATE	lance la mise à jour de l'application
ROLLBACK	annulation de la dernière mise à jour réalisée (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky Anti-Virus)

EXIT	quitter le logiciel (l'exécution de la commande est possible uniquement avec la saisie du mode passe défini via l'interface de l'application)
IMPORT	importation des paramètres de protection de Kaspersky Anti-Virus (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
EXPORT	exporte les paramètres de la protection de l'application

Chaque instruction possède ses propres paramètres, propres à chaque composant de l'application.

DANS CETTE SECTION

Activation de l'application	147
Administration des composants de l'application et des tâches	148
Recherche de virus	150
Mise à jour de l'application	152
Annulation de la dernière mise à jour	153
Exportation des paramètres de protection	153
Importation des paramètres de protection	154
Lancement de l'application	154
Arrêt de l'application	154
Obtention du fichier de trace	154
Consultation de l'aide	155
Codes de retour de la ligne de commande	155

ACTIVATION DE L'APPLICATION

Il est possible d'activer Kaspersky Anti-Virus de deux manières :

- Via Internet à l'aide du code d'activation (commande ACTIVATE) ;
- Via le fichier de clé de licence (commande ADDKEY).

Syntaxe de la commande :

ACTIVATE <code_d'activation>

ADDKEY <nom_du_fichier> /password=< votre_mot_de_passe >

Description des paramètres :

<code d'activation>	Code d'activation de l'application fourni à l'achat de la licence
<nom_du_fichier>	nom de la clé du fichier de licence avec l'extension *.key
<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface

La commande **ADDKEY** ne peut être exécutée sans la saisie préalable du mot de passe.

Exemple

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
```

```
avp.com ADDKEY 1AA111A1.key /password=<votre mot de passe>
```

ADMINISTRATION DES COMPOSANTS DE L'APPLICATION ET DES TACHES

Syntaxe de la commande :

```
avp.com <instruction> <profil|nom_de_la_tâche> [/R[A]:<fichier_de_rapport>]
```

```
avp.com STOP|PAUSE <profil|nom_de_la_tâche> /password=<votre_mot_de_passe>  
[/R[A]:<fichier_de_rapport>]
```

<commande>	L'administration des composants et des tâches de Kaspersky Anti-Virus via la ligne de commande s'opère à l'aide des commandes suivantes : START : lancement du composant de la protection ou de la tâche. STOP : arrêt du composant de la protection ou de la tâche. STATUS : affichage de l'état actuel du composant de la protection ou de la tâche. STATISTICS : affichage des statistiques du composant de la protection ou de la tâche. N'oubliez pas que la commande STOP ne peut être exécutée sans la saisie préalable du mot de passe.
<profil nom_de_la_tâche>	En guise de valeur pour le paramètre <profil>, vous pouvez indiquer n'importe quel composant de la protection en temps réel de Kaspersky Anti-Virus ainsi que les modules qui sont repris dans les composants des tâches d'analyse à la demande ou de mise à jour composées (les valeurs standard utilisées par l'application sont reprises dans le tableau ci-après). En guise de valeur pour le paramètre <nom_de_la_tâche>, vous pouvez indiquer le nom de n'importe quelle tâche d'analyse à la demande ou de mise à jour configurée par l'utilisateur.
<votre_mot_de_passe>	mot de passe d'accès à l'application, défini dans l'interface.
/R[A]:<fichier_de_rapport>	/R:<fichier_de_rapport> : consigner dans le rapport uniquement les événements importants. /RA:<fichier_de_rapport> : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

En guise de valeur pour le paramètre **<profil>**, attribuez une des valeurs suivantes :

RTP	tous les composants de la protection. L'instruction avp.com START RTP lance tous les composants de la protection, si la protection avait été arrêtée. Si le composant a été arrêté via la commande STOP de la ligne de commande, il ne pourra être redémarré via la commande avp.com START RTP. Pour ce faire, il faut exécuter la commande avp.com START <profil> où le paramètre <profil> représente un composant concret de la protection, par exemple avp.com START FM.
pdm	Défense Proactive
FM	Antivirus Fichiers
EM	Antivirus Courrier
WM	Antivirus Internet Valeurs pour les sous-composants d'Antivirus Internet : httpscan (HTTP) : analyse du trafic HTTP ; sc : analyse des scripts.
IM	Antivirus IM ("Chat")
Updater	Mise à jour
Rollback	Annulation de la dernière mise à jour
Scan_My_Computer	Analyse de l'ordinateur
Scan_Objects	Analyse des objets
Scan_Quarantine	Analyse de la quarantaine
Scan_Rootkits	Recherche de la présence éventuelle d'outils de dissimulation d'activité
Scan_Startup (STARTUP)	Analyse des objets de démarrage
Scan_Vulnerabilities (SECURITY)	Recherche de vulnérabilités

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.

Exemples :

➤ Pour activer l'Antivirus Fichiers, saisissez dans la ligne de commande :

```
avp.com START FM
```

➤ Pour rétablir le fonctionnement du contrôle parental, saisissez dans la ligne de commande :

```
avp.com RESUME ParCtl
```

➤ Pour arrêter la tâche d'analyse du poste de travail, saisissez dans la ligne de commande :

```
avp.com STOP Scan_My_Computer /password=<votre_mot_de_passe>
```

RECHERCHE DE VIRUS

La ligne de commande utilisée pour lancer l'analyse antivirus d'un secteur quelconque et pour le traitement des objets malveillants découverts ressemble à ceci :

```
avp.com SCAN [<objet à analyser>] [<action>] [<types de fichiers>] [<exclusions>]
[<fichier de configuration>] [<paramètres du rapport>] [<paramètres complémentaires>]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans l'application en lançant la tâche requise via la ligne de commande. Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface de Kaspersky Anti-Virus.

Description des paramètres :

<objet à analyser> ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
<files>	Liste des chemins d'accès aux fichiers et / ou aux répertoires à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace. Remarques : - mettre le nom de l'objet entre guillemets s'il contient un espace ; - lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
/MEMORY	Objets de la mémoire vive.
/STARTUP	Objets de démarrage.
/MAIL	Boîtes aux lettres.
/REMDRIVES	Tous les disques amovibles.
/FIXDRIVERS	Tous les disques locaux.
/NETDRIVERS	Tous les disques de réseau.
/QUARANTINE	Objets en quarantaine.
/ALL	Analyse du Poste de travail.
/@:<filelist.lst>	Chemin d'accès au fichier de la liste des objets et répertoires inclus dans l'analyse. Le fichier doit être au format texte et chaque nouvel objet doit être mis à la ligne. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi sans guillemets, même s'il contient un espace.
<action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur /i8 .	
/i0	Aucune action n'est exécutée, les informations sont seulement consignées dans le rapport.

/i1	Réparer les objets infectés, si la réparation est impossible, les ignorer.
/i2	Réparer les objets infectés, si la réparation est impossible, supprimer les objets simples; ne pas supprimer les objets infectés au sein d'un conteneur (fichiers composés); supprimer les conteneurs avec un en-tête exécutable (archive sfx).
/i3	Réparer les objets infectés, si la réparation est impossible, supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i4	Supprimer les objets infectés ; supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i8	Confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté.
/i9	Confirmer l'action auprès de l'utilisateur à la fin de l'analyse.
Le paramètre <types de fichiers> définit les types de fichiers qui seront soumis à l'analyse antivirus. Si le paramètre n'est pas défini, seuls seront analysés par défaut les objets pouvant être infectés en fonction du contenu.	
/fe	Analyser uniquement les fichiers qui peuvent être infectés selon l'extension.
/fi	Analyser uniquement les fichiers qui peuvent être infectés selon le contenu.
/fa	Analyser tous les fichiers.
Le paramètre <exclusions> définit les objets exclus de l'analyse. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
-e:a	Ne pas analyser les archives.
-e:b	Ne pas analyser les bases de messagerie.
-e:m	Ne pas analyser les messages électroniques au format plain text.
-e:<filemask>	Ne pas analyser les objets en fonction d'un masque.
-e:<secondes>	Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre <seconds> .
-es:<taille>	Ignorer les objets dont la taille (en Mo) est supérieure à la valeur définie par le paramètre <size> .
Le paramètre <fichier de configuration> définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par le programme pour l'analyse. Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour l'analyse antivirus. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de l'application qui seront utilisées.	
/C:<nom_du_fichier>	Utiliser les valeurs des paramètres définies dans le fichier <nom_du_fichier> .
Le paramètre <paramètres du rapport> définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.	

/R:<fichier_de_rapport>	Consigner uniquement les événements importants dans le fichier indiqué.
/RA:<fichier_de_rapport>	Consigner tous les événements dans le rapport.
<paramètres complémentaires> : paramètres qui définissent l'utilisation de technologies de recherche de virus.	
/iChecker=<on off>	Activer/désactiver l'utilisation de la technologie iChecker.
/iSwift=<on off>	Activer / désactiver l'utilisation de la technologie iChecker.

Exemples :

- *Lancer l'analyse de la mémoire vive, des objets de démarrage automatique, des boîtes aux lettres et des répertoires My Documents, Program Files et du fichier test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents"
"C:\Program Files" "C:\Downloads\test.exe"
```

- *Suspendre l'analyse des objets sélectionnés, lancer une nouvelle analyse de l'ordinateur à la fin de laquelle il faudra poursuivre la recherche d'éventuels virus dans les objets sélectionnés :*

```
avp.com PAUSE Scan_Objects /password=<votre_mot_de_passe>
avp.com START Scan_My_Computer
avp.com RESUME Scan_Objects
```

- *Analyser les objets dont la liste est reprise dans le fichier object2scan.txt. Utiliser le fichier de configuration scan_setting.txt. A la fin de l'analyse, rédiger un rapport qui reprendra tous les événements :*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Exemple de fichier de configuration :

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

MISE A JOUR DE L'APPLICATION

L'instruction pour la mise à jour des modules de Kaspersky Anti-Virus et des bases de l'application possède la syntaxe suivante :

```
avp.com UPDATE [<source_de_la_mise_à_jour>] [/R[A]:<fichier_de_rapport>]
[/C:<nom_du_fichier>] [/APP=<on|off>]
```

Description des paramètres :

<source_de_la_mise_à_jour>	Serveur HTTP, serveur FTP ou répertoire de réseau pour le chargement de la mise à jour. Ce paramètre accepte en tant que valeur le chemin d'accès complet à la source des mises à jour ou une URL. Si le chemin d'accès n'est pas indiqué, la source de la mise à jour sera définie par les paramètres du service de mise à jour de l'application.
/R[A]:<fichier_de_rapport>	/R:<fichier_de_rapport> : consigner dans le rapport uniquement les événements importants. /RA:<fichier_de_rapport> : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.
/C:<nom_du_fichier>	Chemin d'accès au fichier de configuration contenant les paramètres de fonctionnement de Kaspersky Anti-Virus pour la mise à jour.

	Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour la mise à jour de l'application. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs des paramètres définies dans l'interface de l'application qui seront utilisées.
/APP=<on off>	Active / désactive la mise à jour des modules de l'application.

Exemples :

- ➡ *Actualiser les bases de l'application et consigner tous les éléments dans le rapport :*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- ➡ *Mettre à jour les modules de Kaspersky Anti-Virus en utilisant les paramètres du fichier de configuration updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Exemple de fichier de configuration :

```
"ftp://my_server/kav_updates" /RA:avbases_upd.txt /app=on
```

ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de la commande :

```
ROLLBACK [/R[A]:<fichier_de_rapport>][/password=<votre_mot_de_passe>]
```

Description des paramètres :

/R[A]:<fichier_de_rapport>	/R:<fichier_de_rapport> : consigner dans le rapport uniquement les événements importants. /RA:<fichier_de_rapport> : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.
<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface

N'oubliez pas que cette instruction ne s'exécutera pas sans la saisie du mot de passe.

Exemple :

```
avp.com ROLLBACK /RA:rollback.txt/password=<votre mot de passe>
```

EXPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
avp.com EXPORT <profil> <nom_du_fichier>
```

Description des paramètres :

<profil>	Composant ou tâche dont les paramètres sont exportés. Le paramètre <profil> peut prendre n'importe quelle des valeurs indiquées au point "Administration des composants de l'application et des tâches".
-----------------------	---

<nom_du_fichier>	Chemin d'accès au fichier vers lequel sont exportés les paramètres de Kaspersky Anti-Virus. Vous pouvez indiquer un chemin relatif ou absolu. Le fichier de configuration est enregistré au format binaire (<i>dat</i>) si aucun autre format n'est indiqué ou si le format n'est pas précisé et il peut être ensuite utilisé pour transférer les paramètres de l'application vers d'autres ordinateurs. De plus, vous pouvez enregistrer le fichier de configuration au format texte. Dans ce cas, ajoutez l'extension <i>txt</i>. N'oubliez pas que l'importation de paramètres de la protection depuis un fichier texte n'est pas prise en charge. Ce fichier peut être utilisé uniquement pour consulter les paramètres de fonctionnement principaux de Kaspersky Anti-Virus.
------------------	---

Exemple :

```
avp.com EXPORT c:\settings.dat
```

IMPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
avp.com IMPORT <nom_du_fichier> [/password=<votre_mot_de_passe>]
```

<nom_du_fichier>	Chemin d'accès au fichier d'où sont importés les paramètres de Kaspersky Anti-Virus. Vous pouvez indiquer un chemin relatif ou absolu.
<votre_mot_de_passe>	Mot de passe pour Kaspersky Anti-Virus défini via l'interface de l'application. L'importation des paramètres de la protection est possible uniquement depuis un fichier au format binaire.

N'oubliez pas que cette instruction ne s'exécutera pas sans la saisie du mot de passe.

Exemple :

```
avp.com IMPORT c:\settings.dat /password=<mot de passe>
```

LANCEMENT DE L'APPLICATION

Syntaxe de la commande :

```
avp.com
```

ARRET DE L'APPLICATION

Syntaxe de la commande :

```
EXIT /password=<votre_mot_de_passe>
```

<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface
----------------------	---

N'oubliez pas que cette instruction ne s'exécutera pas sans la saisie du mot de passe.

OBTENTION DU FICHIER DE TRACE

La création du fichier de trace s'impose parfois lorsque des problèmes se présentent dans le fonctionnement de Kaspersky Anti-Virus. Il permettra aux spécialistes du service d'assistance technique de poser un diagnostic plus précis.

Syntaxe de la commande :

```
avp.com TRACE [file] [on|off] [<niveau_de_trace>]
```

Description des paramètres :

[on off]	Active / désactive la création d'un fichier de trace
[file]	Recevoir la trace dans un fichier
<niveau_de_trace>	Pour ce paramètre, il est possible de saisir un chiffre compris entre 0 (niveau minimum, uniquement les événements critiques) et 700 (niveau maximum, tous les messages). Lorsque vous contactez le service d'assistance technique, l'expert doit vous préciser le niveau qu'il souhaite. S'il n'a rien recommandé en particulier, il est conseillé de choisir le niveau 500.

Il est conseillé d'activer la création de ces fichiers uniquement pour le diagnostic d'un problème particulier. L'activation permanente de cette fonction peut entraîner une réduction des performances de l'ordinateur et un débordement du disque dur.

Exemples :➡ *Désactiver la constitution de fichiers de trace :*

```
avp.com TRACE file off
```

➡ *Créer un fichier de trace avec le niveau maximum de détails défini à 500 en vue d'un envoi à l'assistance technique :*

```
avp.com TRACE file on 500
```

CONSULTATION DE L'AIDE

Pour consulter l'aide au départ de la ligne de commande, utilisez la syntaxe suivante :

```
avp.com [ /? | HELP ]
```

Pour obtenir de l'aide sur la syntaxe d'une commande particulière, vous pouvez utiliser une des commandes suivantes :

```
avp.com <commande> /?
```

```
avp.com HELP <commande>
```

CODES DE RETOUR DE LA LIGNE DE COMMANDE

Cette rubrique décrit les codes de retour de la ligne de commande. Les codes généraux peuvent être renvoyés par n'importe quelle commande. Les codes de retour des tâches concernent les codes généraux et les codes spécifiques à un type de tâche en particulier.

CODES DE RETOUR GENERAUX	
0	Opération réussie
1	Valeur de paramètre invalide
2	Erreur inconnue

3	Erreur d'exécution de la tâche
4	Annulation de l'exécution de la tâche
CODES DE RETOUR DES TACHES D'ANALYSE ANTIVIRUS	
101	Tous les objets dangereux ont été traités
102	Des objets dangereux ont été découverts

SUPPRESSION DES PROBLEMES

Au cas où des problèmes se présenteraient durant l'utilisation de Kaspersky Anti-Virus, vérifiez si la solution n'est pas décrite dans l'aide ou dans la Banque des solutions de Kaspersky Lab (<http://support.kaspersky.com/fr>). La *banque des solutions* est une rubrique distincte du site du service d'assistance technique qui contient les recommandations sur l'utilisation des produits de Kaspersky Lab ainsi que les réponses aux questions fréquemment posées. Tentez de trouver la réponse à votre question ou la solution à votre problème dans cette ressource.

➡ *Pour consulter la banque de solutions, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique** cliquez sur le lien **Banque de solutions**.

Il existe une autre ressource où vous pouvez obtenir des informations sur l'utilisation des applications : le forum des utilisateurs des applications de Kaspersky Lab. Cette source est également une rubrique distincte du service d'assistance technique. Elle contient les questions, les commentaires et les suggestions des utilisateurs de l'application. Vous pouvez voir les principaux sujets de discussion, envoyer des commentaires sur l'application ou rechercher les réponses à votre question.

➡ *Pour ouvrir le forum des utilisateurs, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Accès direct aux FAQs**.

Si vous ne trouvez pas la solution à votre problème dans l'aide, la banque de solutions ou l'accès direct aux FAQ, nous vous conseillons de contacter le service d'assistance technique de Kaspersky Lab.

DANS CETTE SECTION

Création d'un rapport sur l'état du système	157
Création d'un fichier de trace	158
Envoi des fichiers de données	159
Exécution du script AVZ	159

CREATION D'UN RAPPORT SUR L'ETAT DU SYSTEME

Afin de résoudre vos problèmes, il se peut que les experts du service d'assistance technique de Kaspersky Lab aient besoin d'un rapport sur l'état du système. Ce rapport contient des informations détaillées sur les processus exécutés, les modules et les pilotes chargés, les modules externes de Microsoft Internet Explorer et de l'Assistant Microsoft Windows, les ports ouverts, les objets suspects décelés, etc.

Aucune donnée personnelle relative à l'utilisateur n'est recueillie durant la création du rapport.

➤ *Pour créer un rapport sur l'état du système, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** cliquez sur le bouton **Créer le rapport sur l'état du système**.

Le rapport sur l'état du système est généré aux formats *htm* et *xml* et est enregistré dans l'archive *sysinfo.zip*. Une fois que la collecte des informations sur le système est terminée, vous pouvez consulter le rapport.

➤ *Pour parcourir le rapport, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** cliquez sur le bouton **Voir**.
5. Ouvrez l'archive *sysinfo.zip* contenant les fichiers du rapport.

CREATION D'UN FICHIER DE TRACE

Le système d'exploitation et certaines applications peuvent connaître des échecs après l'installation de Kaspersky Anti-Virus. Dans ce cas, il s'agit généralement d'un conflit entre Kaspersky Anti-Virus et des applications installées ou des pilotes sur l'ordinateur. Afin de résoudre ce problème, les experts du service d'assistance technique de Kaspersky Lab pourraient vous demander de créer un fichier de traçage.

➤ *Pour créer un fichier de trace, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, utilisez la liste déroulante du bloc **Traçages** afin de sélectionner le niveau de traçage. Le niveau de traçage est indiqué par l'expert du service d'assistance technique. En cas d'absence de recommandations du service d'assistance technique, il est conseillé de choisir le niveau **500**.
5. Afin de lancer le traçage, cliquez sur le bouton **Activer**.
6. Reproduisez la situation qui entraîne le problème.
7. Pour arrêter le traçage, cliquez sur le bouton **Désactiver**.

Vous pouvez passer au transfert des résultats du traçage (cf. section "Envoi des fichiers de données" à la page [159](#)) sur le serveur de Kaspersky Lab.

ENVOI DES FICHIERS DE DONNEES

Une fois que les fichiers de traçage et le rapport sur l'état du système ont été créés, il faut les envoyer aux experts du service d'assistance technique de Kaspersky Lab.

Pour charger les fichiers de données sur le serveur du service d'assistance technique, il faut obtenir un numéro de requête. Ce numéro est accessible dans votre Espace personnel sur le site du service d'assistance technique lorsque des requêtes actives sont présentes.

➤ Pour télécharger les fichiers de données sur le serveur du service d'Assistance technique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique**, dans le groupe **Actions** cliquez sur le bouton **Envoyer les informations pour le service d'assistance technique**.
5. Dans la fenêtre qui s'ouvre, cochez les cases en regard des fichiers que vous souhaitez envoyer au service d'assistance technique puis cliquez sur **Envoyer**.
6. Dans la fenêtre ouverte **Saisir le numéro de requête (numéro SRF)** indiquez le numéro attribué à votre requête au moment de remplir le formulaire en ligne sur le site du service d'Assistance technique.

Les fichiers de données sélectionnés seront compactés et envoyés sur le serveur du service d'assistance.

S'il n'est pas possible pour une raison quelconque de contacter le service d'assistance technique, vous pouvez enregistrer le fichier de données sur votre ordinateur.

➤ Pour enregistrer les fichiers de données sur le disque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique**, dans le groupe **Actions** cliquez sur le bouton **Envoyer les informations pour le service d'assistance technique**.
5. Dans la fenêtre qui s'ouvre, cochez les cases en regard des fichiers que vous souhaitez envoyer au service d'assistance technique puis cliquez sur **Envoyer**.
6. Dans la fenêtre **Saisir le numéro de requête (numéro SRF)** cliquez sur le bouton **Annuler** et dans la fenêtre qui s'ouvre, confirmez l'enregistrement des fichiers sur le disque.
7. Dans la fenêtre qui s'ouvre définissez le nom d'archive.

Vous pourrez ensuite envoyer les fichiers enregistrés au service d'assistance technique via l'Espace personnel (<https://my.kaspersky.com/fr/>).

EXECUTION DU SCRIPT AVZ

Les experts de Kaspersky Lab analysent votre problème sur la base du fichier de trace et du rapport sur l'état du système. Cette analyse débouche sur une séquence d'actions à exécuter pour supprimer les problèmes identifiés. Le nombre de ces actions peut être très élevé.

Pour modifier la procédure de résolution des problèmes, des scripts AVZ sont utilisés. Le script AVZ est un ensemble d'instructions qui permettent de modifier les clés du registre, de mettre des fichiers en quarantaine, de lancer des recherches de catégories avec possibilité de mise en quarantaine des fichiers en rapport, de bloquer les intercepteurs UserMode et KernelMode, etc.

Pour exécuter les scripts inclus dans l'application, utilisez *l'Assistant d'exécution des scripts AVZ*. L'Assistant se présente sous la forme d'une succession de fenêtres (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Il est déconseillé de modifier le texte du script envoyé par les experts de Kaspersky Lab. En cas de problème lors de l'exécution du script, contactez le service d'assistance technique..

➡ *Pour lancer l'Assistant, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique** qui s'ouvre, cliquez sur le lien **Outils d'assistance** dans la partie inférieure de la fenêtre.
4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre cliquez sur le bouton **Exécuter le script AVZ**.

Si l'exécution du script réussit, l'Assistant termine. Si un échec se produit durant l'exécution du script, l'Assistant affiche le message correspondant.

REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Déclaration sur la collecte des données

A. INTRODUCTION

VEUILLEZ LIRE CE DOCUMENT ATTENTIVEMENT. IL CONTIENT DES INFORMATIONS IMPORTANTES DONT VOUS DEVEZ PRENDRE CONNAISSANCE AVANT DE CONTINUER À UTILISER NOS SERVICES OU NOTRE LOGICIEL. LA POURSUITE DE L'UTILISATION DU LOGICIEL ET DES SERVICES DE KASPERSKY LAB MARQUE VOTRE ACCEPTATION DE CETTE DÉCLARATION SUR LA COLLECTE DES DONNÉES PAR KASPERSKY LAB. Nous nous réservons le droit de modifier la présente déclaration sur la collecte des données en publiant les changements sur cette page. Veuillez vérifier la date de modification ci-dessous afin de voir si la politique a été amendée depuis votre dernière lecture. La poursuite de l'utilisation de n'importe lequel des services de Kaspersky Lab après la publication d'une déclaration actualisée sur la collecte des données marque votre acceptation des modifications introduites.

Kaspersky Lab et ses partenaires (ci-après « Kaspersky Lab ») ont rédigé cette déclaration sur la collecte des données afin de présenter les pratiques de collecte et de distribution de données pour Kaspersky Anti-Virus et Kaspersky Internet Security.

Propos de Kaspersky Lab

Kaspersky Lab est ouvertement engagée dans l'offre d'un service de qualité supérieure à tous ses clients et nous accordons une attention particulière à vos préoccupations sur la collecte de données. Nous sommes conscients des questions que vous pourriez avoir sur la manière dont Kaspersky Security Network rassemble et utilise les données et les informations et la présente déclaration (la « Déclaration sur la collecte des données » ou la « Déclaration » est née de notre volonté de vous présenter les principes qui régissent la collecte de données dans le cadre de Kaspersky Security Network.

Cette Déclaration sur la collecte des données reprend de nombreux détails généraux et techniques sur les procédures que nous avons mises en place pour répondre à vos préoccupations en la matière. Le présent document a été organisé selon les processus et les domaines afin que vous puissiez accéder rapidement aux informations qui vous intéressent le plus. Sachez que toutes nos actions, y compris la protection de vos données, sont gouvernées par la volonté de répondre à vos besoins et à vos attentes.

Les données et les informations sont recueillies par Kaspersky Lab. En cas de questions ou de doutes sur la collecte de données après la lecture de la présente déclaration, n'hésitez pas à envoyer un message électronique à l'adresse support@kaspersky.com.

Qu'est-ce que le Kaspersky Security Network ?

Le service Kaspersky Security Network permet à tous les utilisateurs des logiciels de sécurité informatique de Kaspersky Lab dans le monde entier de contribuer aux efforts d'identification des nouvelles menaces pour la sécurité de vos ordinateurs et de réduire de cette manière le temps de développement de la riposte adéquate. Afin de pouvoir identifier les nouvelles menaces et leurs sources et dans le but d'améliorer d'une part la sécurité de l'utilisateur et, d'autre part, les fonctions du logiciel, Kaspersky Security Network enregistre des données particulières sur la sécurité et les applications et les transmet à Kaspersky Lab où elles seront analysées. Ces informations ne contiennent aucun élément capable d'établir l'identité de l'utilisateur et elles sont exploitées par Kaspersky Lab dans l'unique but d'améliorer ses logiciels de sécurité et de renforcer les solutions contre les menaces malicieuses et les virus. Au cas où des données personnelles seraient recueillies par accident, Kaspersky Lab s'engage à les protéger conformément aux dispositions de cette Déclaration sur la collecte des données.

Votre participation au Kaspersky Security Network, conjointement aux autres utilisateurs des logiciels de sécurité informatique de Kaspersky Lab dans le monde entier, contribue énormément à la sécurisation d'Internet.

Questions légales

Il se peut que Kaspersky Security Network soit soumis aux lois de plusieurs juridictions dans la mesure où ses services peuvent être utilisés dans des juridictions différentes, y compris aux États-Unis. Kaspersky Lab dévoilera les informations

permettant d'établir votre identité sans votre autorisation dans les situations où la loi l'exige ou lorsqu'elle pense de bonne foi que cette action s'impose dans le cadre d'une enquête sur des activités qui nuisent aux biens, aux invités, aux visiteurs et aux partenaires de Kaspersky Lab ou à d'autres ou afin de les protéger contre les activités nuisibles. Comme nous l'avons déjà dit, la législation applicable aux données et aux informations recueillies dans le cadre du Kaspersky Security Network peut varier selon le pays. Ainsi, certaines données permettant d'établir l'identité d'un individu recueillies dans les États membres de l'Union européenne sont couvertes par les directives européennes relatives aux données personnelles, à la confidentialité et aux communications électroniques telles que la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et les législations ultérieures adoptées par les États membres ou la décision 497/2001/CE de la Commission européenne sur les clauses contractuelles types (transfert de données personnelles vers des pays tiers) et les législations ultérieures adoptées par les États membres de l'Union européenne.

Kaspersky Security Network informera comme il se doit les utilisateurs concernés au début de la collecte des informations citées ci-dessus ou avant de partager ces informations, notamment dans le cadre du développement commercial, et donnera la possibilité à ces utilisateurs d'Internet de marquer leur accord (dans les États membres de l'Union européenne et dans les autres pays qui requiert une procédure de confirmation volontaire) ou le désaccord (pour tous les autres pays) en ligne pour l'utilisation commerciale de ces données et/ou le transfert de celles-ci à des tiers.

Kaspersky Lab peut être obligée par les autorités judiciaires ou de police à fournir aux autorités publiques certaines données permettant d'établir l'identité d'un individu. En cas de demande introduite par les autorités judiciaires ou la police, nous fournirons ces informations dès que nous aurons reçu les documents adéquats. Kaspersky Lab pourra également fournir des informations à la police pour protéger ses biens ainsi que la santé et la sécurité de personnes dans les limites définies par les lois.

Les divulgations aux autorités de protection des données à caractère personnel des États membres seront réalisées conformément aux législations en vigueur dans les États membres de l'Union européenne. Les informations relatives à ces divulgations seront accessibles dans les services de Kaspersky Security Network.

B. INFORMATIONS RECUEILLIES

Les données que nous recueillons

Les utilisateurs ont le droit d'envoyer les données conformément à cette déclaration et le service Kaspersky Security Network est chargé de recueillir des données fondamentales et étendues sur les risques potentiels qui menacent votre ordinateur et de les transmettre à Kaspersky Lab. Ces données reprennent :

Données fondamentales

* Informations sur votre matériel et sur vos logiciels, y compris le système d'exploitation et les services pack installés, les objets du noyau, les pilotes, les services, les extensions Internet Explorer, les extensions d'impression, les extensions Windows Explorer, les fichiers de programme téléchargés, les éléments de configuration actifs, les applets du panneau de configuration, les enregistrements de l'hôte et du registre, les adresses IP, les types de navigateur, les clients de messagerie et le numéro de version du logiciel de Kaspersky Lab qui, en général, ne permettent pas d'établir l'identité ;

* Un identifiant unique généré par le logiciel de Kaspersky Lab pour identifier des machines individuelles sans identifier l'utilisateur et qui ne contient aucune information à caractère personnel ;

* Informations sur l'état de la protection antivirus de votre ordinateur et données sur tout fichier ou activité soupçonné de provenir d'un programme malveillant (exemple : nom de virus, date et heure de la détection, noms/chemin d'accès et taille des fichiers infectés, adresse IP et port de l'attaque de réseau, nom de l'application soupçonnée d'être malveillante). Notez que les données citées ci-dessus ne contiennent pas d'éléments d'information capables d'établir une identité.

Données étendues

* Informations relatives aux applications à signature numérique téléchargées par l'utilisateur (URL, taille de fichier, nom du signataire)

* Informations relatives aux applications exécutables (taille, attributs, date de création, informations sur les en-têtes PE, région, nom, emplacement et utilitaire de compression utilisé).

Fichiers et / ou leurs composants

Kaspersky Security network peut accumuler et confirmer les fichiers entiers et / ou leurs composants à propos de Kaspersky Lab pour l'analyse complémentaire. Le transfert des fichiers et / ou leurs composants est réalisé uniquement si vous avez accepté Kaspersky Lab Data Collection Statement.

Sécurisation de la transmission et du stockage des données

Kaspersky Lab s'engage à assurer la sécurité des données qu'elle recueille. Les informations recueillies sont stockées sur des serveurs auxquels l'accès est limité et contrôlé. Kaspersky Lab utilise des réseaux de données sécurisés protégés par des pare-feu conformes aux normes du secteur et des mots de passe. Kaspersky Lab utilise un large éventail de technologies et de procédures de sécurité pour protéger les informations recueillies contre les menaces telles que l'accès, l'utilisation ou la divulgation non autorisée. Nos politiques de sécurité sont revues à intervalle régulier et améliorées selon les besoins et seuls des individus autorisés ont accès aux données que nous recueillons. Kaspersky Lab veille à ce que vos données soient traitées en toute sécurité et conformément aux dispositions de cette Déclaration. Malheureusement, aucune transmission de données ne peut être sécurisée à 100%. Par conséquent, alors que nous entreprenons tout ce qui est en notre pouvoir pour protéger vos données, nous ne pouvons garantir la sécurité des données que vous nous envoyez depuis nos produits ou services, y compris, et sans limite, via le Kaspersky Security Network, et vous utilisez ces services à vos propres risques.

Les données qui sont recueillies peuvent être transmises aux serveurs de Kaspersky Lab et Kaspersky Lab a adopté les mesures de précaution nécessaire pour veiller à ce que les informations recueillies, si elles sont transmises, jouissent d'un niveau de protection adéquat. Nous traitons les données que nous recevons comme des données confidentielles, c.-à-d. conformément à nos procédures de sécurité et à nos politiques d'entreprise sur la protection et l'utilisation des données confidentielles. Une fois que les données recueillies sont arrivées chez Kaspersky Lab, elles sont stockées sur un serveur doté des mesures de protection physiques et électroniques habituelles dans le secteur, y compris le recours à des procédures d'ouverture de session/mot de passe et des pare-feu électroniques chargés de bloquer tout accès non autorisé depuis l'extérieur de Kaspersky Lab. Les données recueillies par le Kaspersky Security Network et couvertes par cette Déclaration sont traitées et stockées aux Etats-Unis et dans d'autres juridictions et dans d'autres pays où Kaspersky Lab est présente. Tous les employés de Kaspersky Lab connaissent nos politiques de sécurité. Vos données sont accessibles uniquement aux employés qui en ont besoin dans l'exercice de leur fonction. Aucune information stockée ne sera associée à des informations permettant d'établir une identité. Kaspersky Lab n'associe pas les données stockées par le Kaspersky Security Network à d'autres données, des listes de contact ou des informations d'abonnement recueillies par Kaspersky Lab à des fins de promotion ou autres.

C. UTILISATION DES DONNÉES RECUEILLIES

Utilisation de vos informations à caractère personnel

Kaspersky Lab recueille les données afin de les analyser et d'identifier les sources de risques pour la sécurité et dans le but d'améliorer la capacité des logiciels de Kaspersky Lab à détecter les comportements malveillants, les sites frauduleux, les programmes criminels et d'autres menaces présentes sur Internet afin de pouvoir offrir à l'avenir le meilleur niveau de protection possible aux clients de Kaspersky Lab.

Divulgaration des informations aux tiers

Kaspersky Lab peut être amenée à divulguer des informations recueillies suite à une demande d'un représentant de la police si la loi l'exige ou l'autorise, suite à une citation à comparaître ou une autre procédure légale ou si nous croyons, en toute bonne foi, que nous devons agir de la sorte pour respecter la loi en vigueur, des règlements, une citation à comparaître ou d'autres procédures légales ou demandes imposées par les autorités publiques. Kaspersky Lab peut également dévoiler des informations permettant d'établir l'identité d'une personne lorsque nous avons des raisons de penser que la divulgation de ces informations s'impose pour identifier un individu, le contacter ou lancer des poursuites judiciaires contre celui-ci si il viole cette Déclaration, les dispositions du contrat avec la Société ou pour protéger la sécurité de nos utilisateurs et du public ou dans le cadre d'accord de confidentialité et de contrat de licence avec des tiers qui nous aident à développer, à faire fonctionner et à entretenir le Kaspersky Security Network. Afin de promouvoir la prise de conscience des risques que présente Internet et la détection et la prévention de ceux-ci, Kaspersky Lab peut partager certaines informations avec des organismes de recherche ou d'autres éditeurs de logiciels antivirus. Kaspersky Lab peut également utiliser les statistiques tirées des informations recueillies pour suivre les tendances au niveau des risques et rédiger des rapports.

Vos choix

La participation à Kaspersky Security Network est facultative. Vous pouvez activer et désactiver le service Kaspersky Security Network à tout moment dans la section Renvoi d'informations dans la page de configuration de votre logiciel Kaspersky Lab. Notez toutefois que si vous choisissez de désactiver le Kaspersky Security Network, nous ne serons peut-être pas en mesure de vous offrir certains des services qui dépendent de la collecte de ces données. Une fois que la période de service de votre logiciel Kaspersky Lab arrive à échéance, certaines des fonctions du logiciel peuvent continuer à fonctionner mais les informations ne seront pas envoyées automatiquement à Kaspersky Lab.

Nous nous réservons également le droit d'envoyer de temps à autre des messages d'alertes aux utilisateurs afin de les informer des modifications spécifiques qui pourraient avoir un impact sur leur capacité à utiliser les services auxquels ils ont souscrits. Nous nous réservons également le droit de vous contacter si une procédure légale nous y oblige ou si nous avons enregistré une violation des contrats de licence, d'achat ou de garantie.

Kaspersky Lab n'abandonne pas ces droits car en des cas restreints, nous pensons que nous pourrions avoir besoin de vous contacter pour une question légale ou pour d'autres questions qui pourraient être importantes pour vous. Ces droits ne nous autorisent pas à vous contacter pour vous présenter de nouveaux services ou des services existants si vous avez choisi de ne pas être contactés pour ce genre de communication et ce genre de publication est rare.

D. COLLECTE DE DONNÉES - QUESTIONS ET RÉCLAMATIONS

Kaspersky Lab prête la plus grande attention aux préoccupations des utilisateurs sur la collecte de données. Si vous estimez avoir été victime du non-respect de cette Déclaration quant à vos données ou vos informations ou si vous avez des questions, vous pouvez envoyer un courrier électronique à Kaspersky Lab : support@kaspersky.com.

Veuillez détailler le plus possible dans votre message la nature de votre demande. Nous étudierons votre demande ou votre réclamation dans les plus brefs délais.

L'envoi des informations est volontaire. L'option de collecte des données peut être désactivée par l'utilisateur à tout moment dans la rubrique « Renvoi d'informations » de la section « Configuration » du logiciel Kaspersky correspondant.

Copyright © Kaspersky Lab 1997-2009. Tous droits réservés.

UTILISATION D'UN CODE TIERS

Du code développé par des éditeurs tiers a été utilisé dans Kaspersky Anti-Virus.

DANS CETTE SECTION

CryptoEx S.A.R.L.....	166
Bibliothèque fastscript 1.9	166
Bibliothèque pcre 7.4, 7.7.....	166
Bibliothèque GNU bison parser	167
Bibliothèque AGG 2.4	167
Bibliothèque OpenSSL 0.9.8d	167
Bibliothèque Gecko SDK 1.8	169
Bibliothèque zlib 1.2.....	169
Bibliothèque libpng 1.2.8, 1.2.29.....	169
Bibliothèque libnkfm 2.0.5	169
Bibliothèque expat 1.2, 2.0.1	169
Bibliothèque Info-ZIP 5.51	170
Bibliothèque Windows Installer XML (WiX) 2.0.....	170
Bibliothèque passthru.....	173
Bibliothèque filter	173
Bibliothèque netcfg	173
Bibliothèque pcre 3.0	173
Bibliothèque RFC1321-based (RSA-free) MD5 library	174
Bibliothèque Windows Template Library (WTL 7.5)	174
Bibliothèque libjpeg 6b	177
Bibliothèque libungif 3.0	178
Bibliothèque libxdr.....	178
Bibliothèque tiniconv - 1,0.0	179
Bibliothèque bzip2/libbzip2 1.0.5	183
Bibliothèque libspf2-1.2.9.....	184
Bibliothèque Protocol Buffer	184

CRYPTOEX S.A.R.L.

La bibliothèque logicielle de protection des informations (BLPI) "Crypto-Sy", développée par Crypto intervient dans la formation et la vérification de la signature numérique dans Kaspersky Anti-Virus. CryptoEx détient une licence FAPSI (FSB) et un certificat pour BLPI "Crypto-Sy".

Le site de CryptoEx : <http://www.cryptoex.ru>

CryptoEx détient tous les droits exclusifs sur la BLPI.

BIBLIOTHEQUE FASTSCRIPT 1.9

La bibliothèque FastScript copyright © Fast Reports Inc. All rights reserved. a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE PCRE 7.4, 7.7

La bibliothèque pcre 7.4, 7.7 copyright © 1997-2008 University of Cambridge sous licence BSD a été utilisée dans le développement de l'application.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTHEQUE GNU BISON PARSER

La bibliothèque bison parser skeleton 2,3 copyright © GNU Project <http://ftp.gnu.org/gnu/bison/> dans le cadre d'une exclusion spéciale a été utilisée dans le développement de l'application.

As a special exception, you may create a larger work that contains part or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

BIBLIOTHEQUE AGG 2.4

La bibliothèque AGG (Anti-Grain Geometry) 2,4 copyright © 2002-2005 Maxim Shemanarev a été utilisée dans le développement de l'application. All rights reserved, sous licence BSD modifiée.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

BIBLIOTHEQUE OPENSSL 0.9.8d

La bibliothèque OpenSSL 0,9.8d copyright © 1998-2007 The OpenSSL Project a été utilisée dans le développement de l'application. All rights reserved, sous les licences OpenSSL License et Original SSLeay License (<http://www.openssl.org/>).

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved a été utilisée dans le développement de l'application.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

BIBLIOTHEQUE GECKO SDK 1.8

La bibliothèque Gecko SDK 1.8 Copyright © Mozilla Foundation a été utilisée dans le développement de l'application. All rights reserved, sous licence MPL 1,1 (<http://www.mozilla.org/MPL/MPL-1.1.html>). Site Web et lien vers la distribution : http://developer.mozilla.org/en/docs/Gecko_SDK.

BIBLIOTHEQUE ZLIB 1.2

La bibliothèque zlib 1.2 copyright © 1995-2005 Jean-loup Gailly and Mark Adler a été utilisée dans le développement de l'application. All rights reserved sous licence zlib/libpng.

BIBLIOTHEQUE LIBPNG 1.2.8, 1.2.29

La bibliothèque libpng 1.2.8, 1.2.29 copyright © 2004, 2006-2008 Glenn Randers-Pehrson a été utilisée dans le développement de l'application. All rights reserved, sous licence zlib/libpng.

BIBLIOTHEQUE LIBNKF 2.0.5

La bibliothèque libnkfm 2.0.5 Copyright (c) KUBO Takehiro a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE EXPAT 1.2, 2.0.1

La bibliothèque Expat 1,2, 2,0,1 Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. All rights reserved, a été utilisée dans le développement de l'application dans les conditions suivantes :

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTHEQUE INFO-ZIP 5.51

La bibliothèque Info-ZIP 5.51 Copyright (c) 1990-2007 a été utilisée dans le développement de l'application. All rights reserved, sous licence Info-ZIP.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

BIBLIOTHEQUE WINDOWS INSTALLER XML (WiX) 2.0

La bibliothèque Windows Installer XML (WiX) 2.0 Copyright (c) Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved, sous licence CPL 1.0 (<http://sourceforge.net/projects/wix/>).

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEQUE PASSTHRU

La bibliothèque Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE FILTER

La bibliothèque Ndis Sample NDIS Lightweight filter driver Copyright (c) 2004-2005 Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE NETCFG

La bibliothèque Network Configuration Sample Copyright (c) 1997 Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE PCRE 3.0

La bibliothèque pcre 3.0 copyright © 1997-1999 University of Cambridge, sous licence PCRE LICENCE a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE RFC1321-BASED (RSA-FREE) MD5 LIBRARY

La bibliothèque RFC1321-based (RSA-free) MD5 library Copyright (c) 1999, 2002 Aladdin Enterprises a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application. Elle est diffusée sous licence zlib/libpng.

BIBLIOTHEQUE WINDOWS TEMPLATE LIBRARY (WTL 7.5)

La bibliothèque Windows Template Library 7,5 Copyright (c) 2005 Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved, sous licence Common Public license 1.0, <http://sourceforge.net/projects/wtl/>.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
 - i) changes to the Program, and
 - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the

Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEQUE LIBJPEG 6B

La bibliothèque libjpeg 6b copyright (c) 1991-1998, Thomas G. a été utilisée dans le développement de l'application. Lane. All Rights. Elle est utilisée dans les conditions suivantes :

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

BIBLIOTHEQUE LIBUNGIF 3.0

La bibliothèque libungif 3.0 Copyright (c) 1997 Eric S a été utilisée dans le développement de l'application. Raymond. Elle est utilisée dans les conditions suivantes :

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTHEQUE LIBXDR

La bibliothèque libxdr copyright © Sun Microsystems, Inc. a été utilisée dans le développement de l'application dans les conditions suivantes :

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

BIBLIOTHEQUE TINICONV - 1,0.0

La bibliothèque tiniconv – 1.0.0 Copyright (C) Free Software Foundation, Inc. author Roman Rybalko (<http://sourceforge.net/projects/tiniconv/>) sous licence GNU LGPL 2,1 (<http://www.gnu.org/>).

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its

terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code

and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

BIBLIOTHÈQUE BZIP2/LIBBZIP2 1.0.5

La bibliothèque bzip2/libbzip2 1.0.5 a été utilisée dans le développement de l'application. copyright (C) 1996-2007 Julian R Seward. All rights reserved a été utilisée dans le développement de l'application. Elle est utilisée dans les conditions suivantes :

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

BIBLIOTHÈQUE LIBSPF2-1.2.9

La bibliothèque libspf2-1.2.9 Copyright 2005 by Shevek and Wayne Schlitt, all rights reserved, a été utilisée dans le développement de l'application sous les conditions The two-clause BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTHEQUE PROTOCOL BUFFER

La bibliothèque Protocol Buffer Copyright 2008, Google Inc. All rights reserved, diffusée sous la licence New BSD License, a été utilisée dans le développement de l'application.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE

COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

GLOSSAIRE

Liste des masques et URL dont le contenu est jugé fiable par l'utilisateur. L'application de Kaspersky Lab ne recherche pas la présence éventuelle d'objets malveillants dans les pages qui correspondent à un élément de la liste.

ACTIVATION DE L'APPLICATION

La procédure d'activation de l'application consiste à saisir le code d'activation suite à la réception de la licence, ce qui permettra à l'application de définir les privilèges d'utilisation et la durée de validité de la licence.

ANALYSE DU TRAFIC

Analyse en temps réel des données transitant par tous les protocoles (exemple : HTTP, FTP etc.), à l'aide de la dernière version des bases d'objets.

ANALYSE HEURISTIQUE

Technologie d'identification des menaces non reconnues par l'antivirus. Celle-ci permet d'identifier les objets soupçonnés d'être infectés par un virus inconnu ou par une nouvelle modification d'un virus connu.

L'analyseur heuristique permet d'identifier jusqu'à 92% des nouvelles menaces. Ce mécanisme est assez efficace et entraîne rarement des faux-positifs.

Les fichiers identifiés à l'aide de l'analyseur heuristique sont considérés comme des fichiers suspects.

APPLICATION INCOMPATIBLE

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui ne peut être administrée via Kaspersky Administration Kit.

ARCHIVE

Fichier qui contient un ou plusieurs autres objets qui peuvent être des archives.

ATTAQUE DE VIRUS

Tentatives multiples d'infection virale d'un ordinateur.

BASE DES URL DE PHISHING

Liste des URL de sites identifiés par les experts de Kaspersky Lab comme des sites de phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky Lab.

BASE DES URL SUSPECTES

Liste des URL dont le contenu pourrait constituer une menace. La liste est rédigée par les experts de Kaspersky Lab. Elle est actualisée régulièrement et est livrée avec l'application de Kaspersky Lab.

BASES

Les bases de données sont créées par les experts de Kaspersky Lab et elles contiennent une description détaillée de toutes les menaces informatiques qui existent à l'heure actuelle ainsi que les moyens de les identifier et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces sont découvertes. Pour améliorer la qualité de la découverte de menaces, nous vous conseillons de télécharger fréquemment les mises à jour des bases depuis les serveurs de mise à jour de Kaspersky Lab.

BASES DE MESSAGERIE

Bases contenant les messages stockés sur votre ordinateur et possédant un format spécifique. Chaque message entrant/sortant est inscrit dans la base de données de messagerie après sa réception/son envoi. Ces bases sont analysées lors de l'analyse complète de l'ordinateur.

Si la protection en temps réel est activée, les messages entrants/sortants sont directement analysés lors de leur réception/envoi.

BLOPAGE D'UN OBJET

Interdiction de l'accès d'applications tiers à l'objet. L'objet bloqué ne peut être lu, exécuté, modifié ou supprimé.

CERTIFICAT DU SERVEUR D'ADMINISTRATION

Certificat qui intervient dans l'authentification du serveur d'administration lors de la connexion à celui-ci de la console d'administration et de l'échange de données avec les postes client. Le certificat du serveur d'administration est créé lors de l'installation du serveur d'administration et il est enregistré dans le sous-répertoire **Cert** du répertoire d'installation.

COMPTEUR D'EPIDEMIE DE VIRUS

Modèle qui sert à prévenir les utilisateurs en cas de menace d'épidémie de virus. Le compteur d'épidémie de virus renferme un ensemble de paramètres qui déterminent un seuil d'activité de virus, les modes de diffusions et le texte des messages.

COPIE DE SAUVEGARDE

Création d'une copie de sauvegarde du fichier avant sa réparation ou sa suppression et placement de cette copie dans la sauvegarde avec la possibilité de restaurer le fichier ultérieurement, par exemple pour l'analyse avec des bases actualisées.

DEGRE D'IMPORTANCE DE L'EVENEMENT

Caractéristique de l'événement consignée dans le fonctionnement de l'application de Kaspersky Lab. Il existe 14 degrés d'importance :

- Événement critique.
- Refus de fonctionnement.
- Avertissement.
- Information.

Les événements de même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

DOSSIER DE SAUVEGARDE

Le stockage spécial est conçu pour l'enregistrement des copies de sauvegarde des objets, créées avant leur première réparation ou suppression.

DUREE DE VALIDITE DE LA LICENCE

Durée pendant laquelle vous pouvez utiliser toutes les fonctions de l'application de Kaspersky Lab. Généralement, la durée de validité d'une licence est d'une année calendrier à partir de la date d'installation. Une fois que la durée de validité est écoulée, les fonctions de l'application sont bloquées : vous ne pourrez plus actualiser les bases de l'application.

ENREGISTREMENT DES OBJETS EN QUARANTAINE

Mode de traitement d'un objet potentiellement infecté empêchant tout accès à celui-ci et engendrant son déplacement vers le dossier de quarantaine où il est conservé de manière cryptée afin de prévenir toute action malveillante.

ETAT DE LA PROTECTION

État actuel de la protection caractérisé par le niveau de sécurité de l'ordinateur.

EXCLUSION

Objet exclu de l'analyse de l'application de Kaspersky Lab. Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple : un répertoire ou un programme), des processus ou des objets selon un type de menace conforme à la classification de l'encyclopédie des virus. Des exclusions peuvent être définies pour chaque tâche.

FICHIERS COMPACTE

Fichier d'archivage contenant un programme de décompactage ainsi que des instructions du système d'exploitation nécessaires à son exécution.

FICHIER DE LICENCE

Fichier portant l'extension **.key** et qui est votre "clé" personnelle, indispensable au fonctionnement de l'application de Kaspersky Lab. Ce fichier sera inclus dans le logiciel si celui-ci a été obtenu chez un distributeur Kaspersky Lab. En revanche, il vous sera envoyé par email si le produit provient d'une boutique Internet.

FLUX NTFS ALTERNATIFS

Flux de données du système de fichiers NTFS (alternate data streams), prévus pour contenir des attributs complémentaires ou des informations relatives au fichier.

Chaque fichier dans le système de fichiers NTFS présente un ensemble de flux (streams). Un des flux renferme le contenu du fichier que nous pouvons voir une fois que le fichier a été ouvert. Les autres flux (alternatifs) sont prévus pour les méta-informations et garantissent, par exemple, la compatibilité du système NTFS avec d'autres systèmes tels que l'ancien système de fichiers Macintosh - Hierarchical File System (HFS). Les flux peuvent être créés, supprimés, enregistrés séparément, renommer ou lancer comme processus.

Les flux alternatifs peuvent être exploités par des individus mal intentionnés dans le but de dissimuler l'envoi ou la réception de données de l'ordinateur.

INSTALLATION A L'AIDE D'UN SCRIPT DE LANCEMENT

Méthode d'installation à distance des applications de Kaspersky Lab qui permet d'associer le lancement d'une tâche d'installation à distance à un compte utilisateur particulier (ou pour plusieurs comptes). Lorsque l'utilisateur s'enregistre dans le domaine, une tentative d'installation de l'application sur le poste client d'où s'est connecté l'utilisateur est lancée. Cette méthode est conseillée pour l'installation d'applications sur des ordinateurs tournant sous Microsoft Windows 98 / Me.

INTERCEPTEUR

Sous-composant de l'application chargé de l'analyse de certains types de messages électroniques. La sélection d'intercepteurs installés dépend du rôle ou de la combinaison de rôles de l'application.

LICENCE ACTIVE

Licence en cours d'utilisation par l'application de Kaspersky Lab.. La licence détermine la durée de validité du fonctionnement complet de l'application ainsi que la politique de licence de l'application. L'application ne peut avoir qu'une application active à la fois.

LICENCE DE RESERVE

Licence ajoutée pour le fonctionnement de l'application de Kaspersky Lab mais qui n'a pas été activée. La licence complémentaire entre en vigueur lorsque la licence active est arrivée à échéance.

LISTE DES URL ANALYSEES

Liste des masques et des URL soumises obligatoirement à la recherche d'objets malveillants par l'application de Kaspersky Lab.

LISTE NOIRE DES FICHIERS DE LICENCES

Base de données contenant des informations relatives aux clés de licence Kaspersky Lab préalablement bloquées, aux utilisateurs ayant transgressé les dispositions du contrat de licence et aux clés qui ont été émises mais qui, pour une quelconque raison, n'ont pas été vendue ou ont été échangées. Le fichier de la liste noire est indispensable au fonctionnement des applications de Kaspersky Lab. Le contenu du fichier est mis à jour en même temps que les bases.

MASQUE DE FICHIER

Représentation du nom et de l'extension d'un fichier par des caractères génériques. Les deux caractères principaux utilisés à cette fin sont ***** et **?** (où ***** représente n'importe quel nombre de caractères et **?** représente un caractère unique). A l'aide de ces caractères, il est possible de représenter n'importe quel fichier. Attention! le nom et l'extension d'un fichier sont toujours séparés par un point.

MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés des serveurs de mise à jour de Kaspersky Lab.

MISE A JOUR ACCESSIBLE

Ensemble de mises à jour des modules de l'application de Kaspersky Lab qui reprend les mises à jour urgentes rassemblées au cours d'un intervalle de temps défini ainsi que les modifications de l'architecture de l'application.

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de garantir l'actualité de la protection. Dans ce scénario, les bases sont copiées depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur et elles sont installées automatiquement.

MISE A JOUR URGENTE

Mise à jour critique des modules de l'application de Kaspersky Lab.

MODELE DE NOTIFICATION

Modèle utilisé pour signaler la découverte d'objets infectés lors de l'analyse. Le modèle de notification contient un ensemble de paramètres qui définissent l'ordre des notifications, les moyens de diffusion et le texte du message.

MODULES LOGICIELS

Fichiers faisant partie de la distribution de l'application de Kaspersky Lab et responsables de ses principales tâches. Chaque type de tâche réalisée par l'application (Protection en temps réel, Analyse à la demande, Mise à jour) possède son propre module exécutable.. En lançant l'analyse complète depuis la fenêtre principale, vous démarrez le module lié à cette tâche.

NIVEAU DE PROTECTION

Le niveau de protection est l'ensemble de paramètres prédéfinis de fonctionnement du composant.

NIVEAU RECOMMANDE

Niveau de protection qui repose sur les paramètres de fonctionnement définis par les experts de Kaspersky Lab et qui garantit la protection optimale de votre ordinateur. Ce niveau de protection est activé par défaut à l'installation.

OBJET A CONTROLER

Fichier transmis via le protocole HTTP, FTP ou SMTP par le pare-feu et envoyé à l'application de Kaspersky Lab pour analyse.

OBJET DANGEREUX

Objet contenant un virus. Nous vous déconseillons de manipuler de tels objets car ils pourraient infecter votre ordinateur. Suite à la découverte d'un objet infecté, il est conseillé de le réparer à l'aide d'une application de Kaspersky Lab ou de le supprimer si la réparation est impossible.

OBJET INFECTE

Objet contenant un code malveillant : l'analyse de l'objet a mis en évidence une équivalence parfaite entre une partie du code de l'objet et le code d'une menace connue. Les experts de Kaspersky Lab vous déconseillent de manipuler de tels objets car ils pourraient infecter votre ordinateur.

OBJET OLE

Objet uni ou intégré à un autre fichier. L'application de Kaspersky Lab permet de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Excel dans un document Microsoft Office Word, ce tableau sera analysé comme un objet OLE.

OBJET INFECTE POTENTIELLEMENT

Objet qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions **com**, **exe**, **dll**, etc. Le risque d'infection par un code malveillant est très élevé pour ces fichiers.

OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus mais inconnu de Kaspersky Lab. Les objets potentiellement infectés sont identifiés à l'aide de l'analyseur heuristique.

OBJET SUSPECT

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus mais inconnu de Kaspersky Lab. Les objets suspects sont détectés grâce à l'analyseur heuristique.

OBJETS DE DEMARRAGE

Série de programmes indispensables au lancement et au bon fonctionnement du système d'exploitation et des applications installés sur votre ordinateur. Ces objets sont exécutés à chaque démarrage du système d'exploitation. Il existe des virus qui s'attaquent en particulier à ces objets, ce qui peut par exemple provoquer le blocage du système d'exploitation.

PARAMETRES DE L'APPLICATION

Paramètres de fonctionnement de l'application communs à tous les types de tâche, responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres de performance de l'application, les paramètres de création des rapports, les paramètres de la sauvegarde.

PARAMETRES DE LA TACHE

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

PASSERELLE A DEUX CANAUX

Ordinateur doté de deux cartes de réseau, chacune d'entre elles connectée à un réseau différent et transmettant les informations d'un réseau à l'autre.

PORT DE RESEAU

Paramètre des protocoles TCP et UDP déterminant la destination des paquets de données IP transmis vers l'hôte via le réseau et permettant aux divers programmes utilisés sur ce même hôte de recevoir des données indépendamment les uns des autres. Chaque programme traite les données envoyées sur un port bien défini (en d'autres termes, le programme "écoute" ce port).

Certains ports standards sont destinés aux protocoles réseau les plus courants (par exemple, les serveurs Web réceptionnent généralement les données envoyées via le protocole HTTP sur le port TCP 80). Néanmoins, un programme peut utiliser n'importe quel protocole et n'importe quel port. Valeurs possibles: de 1 à 65535.

PORT ENTREE-SORTIE

Utilisé dans les microprocesseurs (par exemple Intel) lors de l'échange de données avec les périphériques. Le port entrée-sortie est comparé à l'un ou l'autre périphérique et permet aux applications de le contacter pour l'échange de données.

PORT MATERIEL

Connexion pour un périphérique matériel quelconque via un câble ou une fiche (port LPT, port série, USB).

PROCESSUS DE CONFIANCE

Processus d'une application dont les opérations sur les fichiers ne sont pas contrôlées par l'application de Kaspersky Lab dans le cadre de la protection en temps réel. Tous les objets lancés, ouverts ou conservés par un processus de confiance ne sont pas analysés.

PROTECTION EN TEMPS REEL

Mode de fonctionnement pendant lequel l'application analyse en temps réel la présence de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, écriture et exécution et recherche la présence éventuelle de menaces. Les objets sains sont ignorés alors que les objets (potentiellement) malveillants sont traités conformément aux paramètres de la tâche (réparation, suppression, mise en quarantaine).

PROTOCOLE

Ensemble de règles clairement définies et standardisées, régulant l'interaction entre un client et un serveur. Parmi les protocoles les plus connus et les services liés à ceux-ci, on peut noter: HTTP (WWW), FTP et NNTP (news).

PROTOCOLE D'INTERNET (IP)

Protocole de base du réseau Internet, inchangé depuis son lancement en 1974. Il exécute les opérations principales liées au transfert de données d'un ordinateur à un autre et est à la base de protocoles plus haut niveau tels que le TCP et l'UDP. Il gère la connexion ainsi que la correction d'erreurs. Grâce à des technologies tels que le NAT et le masquage, il est possible de dissimuler d'importants réseaux privés derrière quelques adresses IP (parfois même derrière une seule adresse). Cela permet de satisfaire la demande sans cesse croissante d'adresses IP dont la plage IPv4 est relativement limitée.

REPARATION DES OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration totale ou partielle des données ou sur le constat de l'impossibilité de réparer les objets. La réparation des objets s'opère sur la base des enregistrements des bases. Une partie des données peut être perdue lors de la réparation.

REPARATION DES OBJETS AU REDEMARRAGE

Mode de traitement des objets infectés utilisés par d'autres applications au moment de la réparation. Il consiste à créer une copie de l'objet infecté, à réparer cette copie et à remplacer l'objet original infecté par cette copie lors du redémarrage suivant de l'ordinateur.

RESTAURATION

Déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un dossier spécifié par l'utilisateur.

SCRIPT

Petit programme informatique ou partie indépendante d'un programme (fonction) écrit, en règle générale, pour exécuter une petite tâche particulière. Ils interviennent le plus souvent lors de l'exécution de programmes intégrés à de l'hypertexte. Les scripts sont exécutés, par exemple, lorsque vous ouvrez certains sites Web.

Si la protection en temps réel est activée, l'application surveille l'exécution des scripts, les intercepte et vérifie s'ils contiennent des virus. En fonction des résultats de l'analyse, vous pourrez autoriser ou bloquer l'exécution du script.

SECTEUR D'AMORÇAGE DU DISQUE

Le secteur d'amorçage est un secteur particulier du disque dur de l'ordinateur, d'une disquette ou d'un autre support de stockage informatique. Il contient des informations relatives au système de fichier du disque ainsi qu'un programme de démarrage s'exécutant au lancement du système d'exploitation.

Certains virus, appelés virus de boot ou virus de secteur d'amorçage, s'attaquent aux secteurs d'amorçage des disques. L'application de Kaspersky Lab permet d'analyser les secteurs d'amorçage afin de voir s'ils contiennent des virus et des les réparer en cas d'infection.

SERVEUR PROXY

Service dans les réseaux informatiques qui permet aux clients de réaliser des requêtes indirectes vers d'autres ressources du réseau. Le client se connecte d'abord au serveur proxy et envoie une requête vers une ressource quelconque (par exemple, un fichier) situé sur un autre serveur. Ensuite, le serveur proxy se connecte au serveur indiqué et obtient la ressource demandée ou récupère la ressource dans son cache (si le serveur proxy possède son propre cache). Dans certains cas, la requête du client ou la réponse du serveur peut être modifiée par le serveur proxy à des fins déterminées.

SERVEURS DE MISES A JOUR DE KASPERSKY LAB

Liste de serveurs HTTP et FTP de Kaspersky Lab d'où l'application peut récupérer les bases et les mises à jour des modules.

SERVICE DE NOMS DE DOMAINE (DNS)

Système partagé de traduction du nom d'hôte (ordinateur ou autre périphérique de réseau) en adresse IP. DNS fonctionne dans les réseaux TCP/IP. Dans certains cas particuliers, DNS peut enregistrer et traiter les requêtes de retour et définir le nom de l'hôte sur la base de son IP (enregistrement PTR). La résolution du nom DNS est généralement l'œuvre d'applications de réseau et non pas des utilisateurs.

SEUIL D'ACTIVITE VIRALE

Nombre d'événements d'un type donné et générés dans un intervalle de temps déterminé qui, une fois dépassé, permettra à l'application de considérer qu'il y a augmentation de l'activité virale et développement d'un risque d'attaque virale. Ce paramètre est d'une importance capitale en cas d'épidémie de virus car il permet à l'administrateur d'anticiper l'attaque.

SOCKS

Protocole de serveur proxy permettant une connexion à deux points entre des ordinateurs du réseau interne et des ordinateurs de réseaux externes.

SUPPRESSION D'UN OBJET

Mode de traitement de l'objet qui entraîne sa suppression physique de l'endroit où il a été découvert par l'application (disque dur, répertoire, ressource de réseau). Ce mode de traitement est recommandé pour les objets dangereux dont la réparation est impossible pour une raison quelconque.

TACHE

Fonctions exécutées par l'application de Kaspersky Lab sous la forme d'une tâche, par exemple : **Protection en temps réel des fichiers**, **Analyse complète de l'ordinateur**, **Mise à jour des bases**.

TECHNOLOGIE iCHECKER

Technologie qui permet d'accélérer l'analyse antivirus en excluant les objets qui n'ont pas été modifiés depuis l'analyse antérieure pour autant que les paramètres de l'analyse (bases antivirus et paramètres) n'aient pas été modifiés. Ces informations sont conservées dans une base spéciale. La technologie est appliquée aussi bien pendant la protection en temps réel que dans les analyses à la demande.

Admettons que vous possédez une archive qui a été analysée par une application de Kaspersky Lab et qui a reçu l'état *sain*. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases antivirus, l'archive sera analysée à nouveau.

Limitations technologiques d'iChecker :

- la technologie ne fonctionne pas avec les fichiers de grande taille car dans ce cas il est plus rapide d'analyser tout le fichier que de vérifier s'il a été modifié depuis la dernière analyse ;
- la technologie est compatible avec un nombre restreint de formats (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

TITRE

L'information, qui est contenue dans le début du fichier ou du message, se compose des données de faibles niveaux selon l'état et le traitement du fichier (message). En particulier, l'en-tête du courrier électronique contient des renseignements, tels que, les données de l'expéditeur, du destinataire et la date.

VIRUS DE DEMARRAGE

Virus affectant les secteurs d'amorçage du disque de l'ordinateur. Au redémarrage du système, le virus force le système à inscrire en mémoire et à exécuter du code malveillant au lieu du code d'amorçage original.

VIRUS INCONNU

Nouveau virus pour lequel aucune information ne figure dans les bases. En règle générale, les virus inconnus sont découverts dans les objets à l'aide de l'analyse heuristique et ces objets reçoivent l'état potentiellement infecté.

QUARANTAINE

Répertoire défini dans lequel sont placés tous les objets potentiellement infectés découverts pendant l'analyse ou par la protection en temps réel.

CONTRAT DE LICENCE

Notice importante pour tous les utilisateurs vous devez lire attentivement cette Licence d'utilisation avant de commencer à utiliser ce Logiciel.

En appuyant sur le bouton d'acceptation, vous acceptez les termes et conditions de la Licence. Par cet acte, vous marquez votre volonté de devenir partie à cette Licence.

SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, ANNULEZ L'INSTALLATION DU LOGICIEL ET NE L'INSTALLEZ PAS.

En appuyant sur le bouton d'acceptation, vous avez le droit d'utiliser ce Logiciel en conformité avec tous les termes et conditions de cette Licence.

1. Définitions

1.1. **Logiciel** est défini comme le logiciel, le manuel d'utilisateur, les documents explicatifs et autres, y compris les Mises à jour.

1.2. **Titulaire** des droits (titulaire de tous les droits, exclusifs ou autres liés au Logiciel) est Kaspersky Lab ZAO, une société de droit russe.

1.3. **Ordinateur(s)** signifie l'ordinateur (s) ou hardware (s), et notamment les ordinateurs personnels, ordinateurs portables ou "lap tops", stations de travail, assistants électroniques personnels, téléphones portables mini – ordinateurs ou "smart phones" et tout autre environnement pour lequel le Logiciel a été élaboré et dans lequel il doit être installé.

1.4. **Utilisateur final (Vous)** signifie toute personne qui installe ou qui utilise ce Logiciel dans son ordinateur ou qui en fait une copie légalement, ou, si ce Logiciel a été téléchargé ou installé au nom d'une entreprise, en tant qu'un employeur par exemple, VOUS signifie l'entreprise pour laquelle ce Logiciel a été téléchargé et installé. Selon cette Licence l'entreprise a autorisé l'individu à accepter les termes et conditions de cette Licence en son nom. Sous le terme d'entreprise nous comprenons sans limitation les partenariats de tous types y compris de sociétés de personnes, les sociétés à responsabilité limitée, les associations, les sociétés par action, les joint-ventures, les syndicats et/ou autorités gouvernementales.

1.5. **Partenaire(s)** signifie(nt) l'entreprise(s) ou l'individu(s) qui distribue(nt) ce Logiciel, sur la base d'un accord avec le Titulaire.

1.6. **Mise(s) à jour** signifie(nt) toutes les mises à jour, révisions, retouches, améliorations, modifications, copies, compléments ou paquets de données de maintenance etc.

2. Objet de la licence

2.1. Le Titulaire Vous accorde une licence non-exclusive pour le stockage, le chargement, l'installation, visualisation et l'utilisation de ce Logiciel sur une quantité limitée d'ordinateurs pour protéger votre propre ordinateur, sur lequel le Logiciel est installé, contre les menaces décrites dans le manuel d'utilisation selon les termes et conditions de cet Accord (« Licence ») et à condition que Vous acceptiez la Licence.

Version d'essai: Si Vous avez reçu, téléchargé et/ou installé la version d'essai de ce Logiciel et possédez la Licence pour son évaluation, Vous ne pouvez utiliser ce Logiciel que pour évaluer la proposition et seulement pendant la période d'essai à moins que d'autres conditions existent, à compter de la date de la première installation. Toute autre utilisation de ce Logiciel pour d'autres buts ou après la période d'essai est strictement interdite.

Logiciel à environnement multiple, Logiciel de Langue Multiple, Logiciel de Media à double usage, Copies Multiples, Lots et Paquets de données.

Si Vous utilisez différentes versions du Logiciel ou différentes versions linguistiques, si Vous avez reçu le Logiciel sur divers supports, ou si Vous avez reçu plusieurs copies du Logiciel ou si le Logiciel est lié à d'autres logiciels, le nombre d'utilisateurs autorisés sur les ordinateurs desquels le Logiciel est installé doit correspondre au nombre de Licences reçues de la part du Titulaire, sachant qu' à moins qu'il n'en soit prévu autrement, chaque Licence achetée Vous permet d'installer et d'utiliser le Logiciel tel que spécifié aux points 2.2. et 2.3. de cette Licence.

2.2. Si le Logiciel a été acheté dans un espace de vente sur un support matériel, Vous pouvez utiliser le Logiciel pour protéger le nombre d'ordinateurs mentionné sur le conditionnement.

2.3. Si le Logiciel a été téléchargé sur internet, Vous pouvez l'utiliser afin de protection de la quantité des ordinateurs indiquée lors de l'acquisition du Logiciel,

2.4. Vous avez le droit de faire une copie du Logiciel aux seules fins de sauvegarde et seulement pour remplacer des copies légales qui auraient été perdues, détruites ou devenues inutilisables. Cette copie de sauvegarde ne peut pas être utilisée pour d'autres buts et doit être détruite si Vous perdez le droit de l'utiliser ou à l'échéance du terme de la Licence ou pour tout autre événement selon les lois du pays où Vous habitez à titre principal ou du pays où Vous utilisez ce Logiciel. Vous pouvez transmettre cette Licence non-exclusive d'utilisation du Logiciel à un autre individu ou à d'autres entités juridiques à condition que le destinataire accepte d'être tenu par les termes et conditions de la Licence et qu'il se substituera totalement à Vous. Si Vous transmettez complètement les droits pour l'utilisation du Logiciel, Vous devez détruire toutes les copies et notamment celle de sauvegarde. Si vous êtes le destinataire d'une Licence cédée Vous devez consentir à respecter tous les termes et conditions de cette Licence. Si Vous n'êtes pas d'accord avec les termes et conditions de cette Licence, Vous ne devez pas installer et/ou utiliser ce Logiciel sur votre ordinateur. Vous consentez au titre de destinataire de la Licence cédée à ce que Vous ne déteniez pas de droits supplémentaires ou meilleurs que ceux détenus auparavant par l'acheteur d'origine auprès du Titulaire.

2.5. Du temps de l'activation du Logiciel (à l'exception de la version d'essai) Vous disposez des droits aux services présentés sur le conditionnement du Logiciel (si Vous avez acheté le Logiciel sur un support matériel) ou spécifié lors de l'achat (si Vous avez acheté le Logiciel via internet en version téléchargée) :

- les Mises à jour du Logiciel via internet, quand le Titulaire les à mises sur son propre site officiel ou via d'autres sites en ligne. Toutes autres mises à jour que Vous pourriez recevoir deviennent parties du Logiciel et tous les termes et conditions s'y appliquent.

- Maintenance technique via Internet ou via un service d'assistance technique par téléphone (hotline).

3. Activation et Durée.

3.1. Si Vous modifiez votre ordinateur ou faites des modifications sur d'autres Logiciels installés sur l'ordinateur, Vous pouvez vous voir réclamer par le Titulaire de répéter le processus d'activation du Logiciel. Le Titulaire se réserve le droit d'utiliser tous moyens et processus de vérification la validité de la Licence et/ou la légalité de la copie du Logiciel, installé et/ou utilisé par Vous sur votre ordinateur.

3.2. Si le Logiciel a été acheté sur un support physique, la validité de la Licence court à compter de l'acceptation de celle-ci, pour une période mentionnée sur le conditionnement.

3.3. Si le Logiciel a été téléchargé sur internet, le Logiciel peut être utilisé après la réception de cette Licence qui court à compter de l'achat de la Licence.

3.4. Vous disposez du droit d'utiliser la version d'essai du Logiciel selon les conditions mentionnées dans le point 2.1 et sans aucune obligation pendant période d'essai, qui court à compter de son activation, cette version ne donnant pas droit aux Mises à jours et à la maintenance technique via l'internet ou au service d'assistance technique par téléphone.

3.5. Votre License est limitée par la durée mentionnée aux points 3.2. et 3.3. (si applicable) et la période restante de validité peut être connue dans l'interface graphique d'utilisateur du Logiciel.

3.6. Sans préjudice de toute autre voie de recours en droit ou en équité que le Titulaire pourrait détenir, en cas de violation par Vous-même des termes et conditions de cette Licence, le Titulaire peut, à tout moment et sans aucune information préalable, Vous signifier la résiliation de la Licence sans remboursement du prix d'achat ou de toute partie de celui-ci.

3.7. Vous consentez que dans l'utilisation du Logiciel et dans l'utilisation de tout rapport ou des informations provenant de l'utilisation de ce Logiciel, Vous devez vous conformer à toutes réglementations et législations internationales, nationales, étatiques, régionales et locales, y compris, et sans limitation, en matière de protection de la vie privée, droit d'auteur, contrôle des exportations et des bonnes mœurs.

3.8. Sauf disposition contraire expressément prévue par cette Licence, Vous ne pouvez transmettre ou céder les droits qui Vous sont accordés en vertu de la présente Licence ou l'une des obligations en vertu de cette Licence.

4. Assistance technique.

L'Assistance technique décrite dans le point 2.5. de cette Licence Vous est fournie quand la dernière Mise à jour du Logiciel a été installée (à l'exception de la version d'essai du Logiciel).

5. Collecte des données

5.1. Après avoir accepté les termes et conditions de la présente Licence, Vous consentez à fournir des informations au Titulaire sur les fichiers exécutables et sur leur contrôle afin d'améliorer votre niveau de protection.

5.2. Pour améliorer la sensibilisation de la sécurité aux nouvelles menaces et leurs sources et pour améliorer votre niveau de sécurité, le Titulaire, avec votre consentement, ce qui est confirmé explicitement dans la Kaspersky Security Network Data Collection Statement, est habilité à recevoir de telles informations. Dès lors Vous pouvez désactiver ou activer le Kaspersky Security Network Service à tout moment dans la page des options du Logiciel.

Vous reconnaissez et acceptez que toute information collectée par le Titulaire puisse être utilisée pour poursuivre et rapporter les menaces à la sécurité par le Titulaire et à sa seule discrétion.

5.3. Le Logiciel ne traite aucune donnée nominative et ne combine pas de telle donnée avec des informations personnelles.

5.4. Si Vous ne désirez pas que l'information soit collectée par le Logiciel pour être envoyée au Titulaire, Vous ne devez pas activer et/ou désactiver le Kaspersky Security Network Service.

6. Restriction

6.1. Vous ne devez pas émuler, cloner, louer, prêter, vendre, modifier, décompiler ou désassembler ou créer des produits dérivés sur la base du Logiciel ou sur toute partie, à la seule exception d'un droit non-transférable qui Vous serait accordé par la législation applicable. Vous ne devez pas transmettre la version réduite accessible pour l'utilisation ou transmettre la Licence pour le Logiciel ou d'autres paramètres de la Licence du Logiciel, et il est interdit de le faire par un tiers. Toutes les limitations sont protégées par la loi. Ni le Logiciel en code binaire ni le code source ne peuvent être utilisés pour faire de l'ingénierie amont ou inversée, afin de recréer le programme, qui demeure une propriété privée. Tous les droits, qui ne sont pas prévus de manière expresse dans ce document, sont réservés par le Titulaire et/ou par ses fournisseurs. Toute utilisation non autorisée de ce Logiciel doit être immédiatement terminée en conformité avec la Licence et des actions judiciaires pénales et/ou civiles peuvent être engagées contre Vous-même.

6.2. Vous ne devez pas transmettre les droits de l'utilisation de ce Logiciel à des tiers, à l'exception des cas visés au point 2.4. de cet Accord.

6.3. Vous ne devez pas transmettre le code d'activation et/ou le fichier de clé à des tiers ou permettre aux tiers d'utiliser le code d'activation et/ou le fichier de clé de la Licence, qui sont des données confidentielles du Titulaire. Vous devez garder avec précaution le code d'activation et/ou le fichier de clé de la Licence, même dans le cas de cession à des tiers dans les conditions visées au point 2.4. de cet Accord.

6.4. Vous ne pouvez pas louer, consentir droit à bail ou prêter le Logiciel à des tiers.

6.5. Vous ne devez pas utiliser ce Logiciel pour la création de données ou de logiciel utilisés pour la destruction, le blocage ou la création des menaces décrites dans le manuel d'utilisation.

6.6. Le Titulaire dispose du droit de bloquer la clé ou de cesser votre Licence en cas de violation par Vous-même des termes et conditions, sans aucun délai de prévenance.

6.7. Si Vous utilisez la version d'essai du Logiciel, Vous ne disposez pas du droit de recevoir le support technique décrit au point 4 et Vous ne disposez pas du droit de transmettre la Licence ou ses droits d'utilisation du Logiciel à des tiers.

7. Responsabilité et garantie limitées

7.1. Le Titulaire garantit que le Logiciel répondra conformément aux caractéristiques et la description mentionnés dans le manuel d'utilisation, à condition cependant qu'une telle garantie ne s'applique pas aux cas suivants: (w) défauts de votre ordinateur liées à des carences pour lesquelles le Titulaire refuse expressément devoir engager sa responsabilité ; (x) mauvais fonctionnement, défauts ou pannes résultant d'une mauvaise utilisation, d'abus ; d'accident ; négligence, de mauvaise installation, de fonctionnement ou d'entretien, de vol, de vandalisme, de force majeure, d'actes de terrorisme, de pannes ou de surtensions électriques; de modification interdite ou de réparation par un tiers (autre que le Titulaire) ou par toutes autres actions ou conséquences de Vous-même qui ne relèvent pas du Titulaire ; (y) tout défaut que Vous n'avez pas révélé au Titulaire dans les meilleurs délais à compter de leur première apparition ; et (z) toute incompatibilité causée par un périphérique et/ou logiciel installé sur votre ordinateur.

7.2. Vous avez pris connaissance et acceptez qu'aucun Logiciel ne puisse être libre d'erreurs et la raison pour laquelle Vous êtes invité à faire des copies de sauvegarde à votre convenance et de manière fréquente et fiable.

7.3. Le Titulaire ne donne aucune garantie que le Logiciel puisse fonctionner correctement en cas de violation des conditions indiquées dans le manuel d'utilisation ou dans cet Accord de Licence.

7.4. Le Titulaire ne peut garantir que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour mentionnées aux points 2.5. de cet Accord.

7.5. Le Titulaire ne peut garantir de protection contre les menaces décrites dans le manuel d'utilisation après l'expiration de la période décrite aux points 3.2. et 3.3. de cet Accord ou après l'expiration de la Licence quelle qu'en soit la raison.

7.6. Le Logiciel est fourni "en l'état " et le Titulaire ne donne aucune garantie de passif, et ne donne aucune autre garantie quant à son utilisation ou sa performance. A l'exception de toute garantie de passif, condition, présentation ou durée qui ne peut pas être exclue ou limitée par la loi applicable, le Titulaire et ses partenaires ne donnent aucune garantie, condition, représentation ou durée (expresse ou implicite, quelle qu'en soit le droit applicable) pour toutes les questions y compris, sans limitation, la non violation des droits des tiers, la qualité marchande, la satisfaction, l'intégration et la possibilité de l'usage particulier. Vous assumez toutes les incorrections et tous les risques liés au choix du Logiciel pour atteindre vos résultats attendus ainsi que pour son installation, l'utilisation et les résultats venant de l'utilisation du Logiciel.

Sans limitation des dispositions ci-dessus, le Titulaire ne donne aucune garantie de passif et ne donne aucune garantie que le Logiciel soit exempté d'erreurs, d'interruptions ou d'autres défaillances ou que le Logiciel corresponde à une ou toutes vos attentes, qu'elles soient ou non connues du Titulaire.

8. Exclusion et limitation de responsabilité

8.1. Dans la mesure où cela est autorisé par la loi, en aucun cas le Titulaire et ses partenaires ne seraient être responsables des dommages occasionnels, épisodiques, des dommages et intérêts indirects quels qu'ils soient (y compris, mais sans limitation, les dommages pour perte de profit ou de données confidentielles et toute autre information, les dommages liés à la perte d'opportunités commerciales, de données personnelles, pour corruption, atteinte ou perte de données et programmes, pour NON-RESPECT DE toute obligation, y compris une obligation légale, une obligation de bon foi ou une obligation de diligence raisonnable, les pertes pour cause de négligence, pertes économiques ou toutes autres pertes quelles qu'elles soient) étant la conséquence ou concernant l'impossibilité d'utiliser le logiciel, la possibilité de fournir l'assistance technique, ou d'autres services, informations ou programmes en liaison avec l'utilisation du Logiciel, ou découlant du non respect des obligations contractuelles, faute (y compris les négligences, les perturbations, les autres violations sérieuses des obligations et des charges) et ce concernant toutes les autres violations de garanties données par le Titulaire ou ses Partenaires qui ont été prévues de la possibilité d'existence de tels dommages.

Vous consentez que dans le cas où le Titulaire ou/et ses Partenaire supportent la responsabilité, cette responsabilité sera limitée au montant du prix du Logiciel. La responsabilité ne peut pas dépasser la somme dépensée pour l'achat du Logiciel auprès du Titulaire ou ses représentants ou partenaires.

Rien dans cet Accord exclut ou limite toute action pour décès ou dommages corporels.

Par ailleurs si aucune réserve, exclusion ou limitation ne peut être exclue ou limitée au regard du droit applicable, ses réserves, exclusions ou limitations ne Vous seront pas applicables mais Vous serez tenu par toutes les réserves, exclusions et limitations restantes exprimées dans cet Accord.

9. Licence des programmes informatiques mis à disposition des utilisateurs en tant que Logiciels Libres (GNU General Public Licence) et autres licences

Le Logiciel peut inclure des programmes informatiques mis à disposition des utilisateurs sur le fondement de contrats de licence ou de contrats de sous- licences et tant que Logiciels Libres (GNU General Public Licence - GPL) ou autre licences de logiciels libres similaires, qui entre autres droits consentis, permettent à l'utilisateur de copier, modifier ou re –distribuer certains programmes, ou leur parties et d'avoir le droit d'accéder au code – source (Open Source Software).

Si ces licences requièrent pour ce type de Logiciels qui sont mis à disposition en format binaire exécutable, que le code source des logiciels distribués soit également disponible aux autres utilisateurs, dans ce cas la demande afin d'obtenir le code source doit être faite à l'adresse suivante : source@kaspersky.com. Si un programme informatique mis à disposition des utilisateurs en tant que Logiciel Libre et qui permet à l'utilisateur de copier, modifier ou re –distribuer certains programmes, ou leur parties et d'avoir le droit d'accéder au code – source (Open Source Software), requiert que le Titulaire fournisse les droits d'accès au code source qui sont plus limités par rapport aux droits prévus dans cet Accord, les droits plus limités l'emportent par aux droits prévus dans cet Accord.

10. Droits de propriété intellectuelle.

10.1. Vous consentez à ce que le Logiciel et le droit d'auteur, les systèmes, les idées, les méthodes, la documentation et l'information contenus dans le Logiciel relèvent de la propriété intellectuelle et/ou du secret commercial du Titulaire ou de ses Partenaire et que le Titulaire et ses Partenaires soient notamment protégés par les lois civiles et pénales, sur le droit d'auteur, le secret des affaires, les marques et brevets de la Fédération de la Russie, de l'Union Européenne, des Etats-Unis et d'autres pays et traités internationaux.

Cet Accord ne vous accorde pas de droit en matière de propriété intellectuelle, notamment au regard des marques de commerce ou de marques de service qui appartiennent au Titulaire ou/et à ses Partenaires (« les Marques »). Vous pouvez utiliser les Marques pour identifier le résultat issu du Logiciel, en conformité avec la pratique universellement admise en la matière, y compris l'identification du Propriétaire des « Marques ». Cette utilisation de la Marque ne vous confère pas de droit de propriété sur la Marque.

Le Titulaire et/ou ses partenaires possèdent et conservent tous les droits, titres et les intérêts relatifs au Logiciel, y compris et sans limitation les corrections de fautes, les renforcements, les Mises à jour et autres modification du Logiciel, causés par le Titulaire ou par des tiers, tous les droits d'auteur et les secrets commerciaux, les brevets, les marques de commerce et d'autre droits de propriété intellectuelle déjà mentionnés.

La possession, l'installation et l'utilisation du Logiciel ne Vous donnent et ne Vous donneront aucun droit de propriété intellectuelle sur le Logiciel, sauf ceux expressément mentionnés dans le présent Accord. Toutes les copies du Logiciel doivent contenir la mention du propriétaire à savoir le nom du Titulaire. La Licence ne Vous donne pas droit de Propriété intellectuelle pour le Logiciel et vous acceptez que la Licence Vous permette seulement d'utiliser le Logiciel selon les termes et conditions décrits. Le Titulaire conserve tous les droits qui n'ont pas été accordés par le présent Accord.

10.2. Vous acceptez que le code source, le code d'activation et/ou la clé de la Licence pour ce Logiciel demeure la Propriété du Titulaire et constituent un secret commercial pour celui-ci. Vous consentez à ne pas modifier, adapter, traduire, décompiler et accéder au code source du Logiciel de quelque manière que ce soit.

10.3. Vous donnez votre accord pour ne pas modifier ou détériorer le Logiciel. Vous ne pouvez pas déplacer ou changer les mentions écrites relative à l'identité du détenteur des droits de la propriété intellectuelle ou toute autre information relative au propriétaire sur les copies du Logiciel.

11. Législation applicable. Arbitrage

Cet Accord est régi par les seules lois de la Fédération de Russie, et non par la Convention des Nations Unies sur les Contrats Internationaux de vente de biens. Tous les conflits concernant l'interprétation des clauses de cet Accord ou toutes autres violations, s'ils ne sont pas résolus à l'amiable par les parties, relèvent de la compétence du Tribunal

d'arbitrage commercial international de la chambre de commerce et d'industrie de la ville de Moscou, en Fédération de Russie. Chaque jugement rendu par l'arbitre s'imposera aux parties, et tout autre jugement concernant le premier jugement peut être exécuté par les tribunaux ayant compétences dans les autres juridictions concernées.

Aucune disposition du présent article 11 ne saurait empêcher une partie de rechercher et obtenir un procès équitable d'un tribunal compétent, que ce soit avant, pendant ou après la procédure arbitrale.

12. Délai pour ester en justice

Toutes actions en justice relatives à cet Accord doivent être intentée par la partie concernée dans les l'année à compter de la date de leur constat ou de leur découverte, à l'exception de celle relative à une violation des droits de propriété intellectuelle qui peuvent intervenir dans les délais maximum prévus par la législation applicable.

13. Intégralité du contrat, autonomie des clauses du contrat, absence de renonciation

Cet Accord exprime l'intégralité des obligations entre Vous et le Titulaire et prévaut sur tout autre accord antérieur, proposition, communication que ce soit oral ou écrit, relatif au Logiciel ou aux sujets évoqués dans le présent Accord de Licence. Vous reconnaissez en avoir eu connaissance, le comprendre et consentez à en respecter les termes.

Si une des dispositions de ce contrat venait à être considérée comme nulle, incomplète ou non valide en intégralité ou en partie par un tribunal, celle-ci devra être modifiée ou restreinte pour être rendue conforme à la législation en vigueur afin de devenir applicable, et cet Accord sera applicable en en intégralité dans les limites permises par la législation en vigueur tout en préservant son objet et but initiaux.

Aucune renonciation à n'importe quelle provision de cet Accord ne peut être réputée valide sauf si elle est précisée sous forme écrite par Vous et par le Représentant autorisé du Titulaire en prenant en compte qu'aucune renonciation qui précède la renonciation fixée par les parties ne sera applicable.

L'absence d'action de la part du Titulaire afin d'appliquer de manière forcée toute provision de cet Accord, ne saurait être interprétée comme une renonciation à ses droits.

14. Information contact

Si vous avez des questions concernant cet Accord ou si vous désirez joindre les services du Titulaire, vous pouvez le faire en vous adressant à:

Kaspersky Lab, 10/1 1 st Volokolamsky Proezd

Moscou, 123060

Fédération de la Russie

Tel: + 7-495-979-8700,

Fax: + 7-495-645-7939

Email: info@kaspersky.com

Website: www.kaspersky.com

2009 Kaspersky Lab ZAO. Tous droits réservés. Le Logiciel et sa documentation sont protégés par les droits d'auteur ainsi que par les autres droits de propriété intellectuelle, traités internationaux en la matière, et autres lois concernant la protection des droits de propriété intellectuelle.

KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux Etats-Unis (Californie). Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les experts principaux de Kaspersky Lab siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malfaisants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus® : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous élaborons, mettons en œuvre et accompagnons les dispositifs de protection antivirale pour entreprise. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez des réponses complètes à vos questions.

Site Web de Kaspersky Lab : <http://www.kaspersky.com/fr>

L'Encyclopédie des virus : <http://www.viruslist.com/fr>

Laboratoire antivirus : <http://newvirus.kaspersky.fr>

Forum de Kaspersky Lab : <http://forum.kaspersky.com>

INDEX

A

Algorithme de fonctionnement	
Antivirus Courrier	53
Antivirus Fichiers	43
Antivirus IM ("Chat")	67
Antivirus Internet	60
Analyse	
action sur l'objet sélectionné	77
analyse des fichiers composés	79
compte utilisateur	81
lancement	74
lancement automatique de la tâche ignorée	81
niveau de protection	76
optimisation de l'analyse	78
planification	81
recherche de vulnérabilités	82
technologies d'analyse	80
type d'objets analysés	77
Analyse heuristique	
Antivirus Courrier	56
Antivirus Fichiers	46
Antivirus IM ("Chat")	68
Antivirus Internet	64
Antivirus Courrier	
algorithme de fonctionnement	53
analyse des fichiers composés	57
analyse heuristique	56
filtrage des pièces jointes	57
niveau de protection	53
réaction face à la menace	54
restauration des paramètres par défaut	58
zone de protection	55
Antivirus Fichiers	
algorithme de fonctionnement	43
analyse des fichiers composés	47
analyse heuristique	46
mode d'analyse	48
niveau de protection	44
optimisation de l'analyse	46
réaction face à la menace	44
restauration des paramètres par défaut	51
suspension du fonctionnement	49, 50
technologie d'analyse	48
zone de protection	45
Antivirus IM ("Chat")	
algorithme de fonctionnement	67
analyse heuristique	68
base des URL de phishing	67
zone d'analyse	67
Antivirus Internet	
algorithme de fonctionnement	60
analyse heuristique	64
base des URL de phishing	62
module d'analyse des liens	63
niveau de protection	61
optimisation de l'analyse	64
réaction face à la menace	61
zone de protection	62

Autodéfense du logiciel	102
-------------------------------	-----

B

Base des URL de phishing	
Antivirus IM ("Chat")	67
Antivirus Internet	62

C

Catégories de menaces identifiées	106
Clavier virtuel.....	121
Composants du programme	15
Configuration du navigateur	124
Copie de sauvegarde	187

D

Défense Proactive	
contrôle des comptes utilisateur système	71
liste des activités dangereuses.....	69
règle de contrôle de l'activité dangereuse.....	70
Désactivation/activation de la protection en temps réel.....	95
Disque de dépannage	122
Dossier de sauvegarde	116

F

Fenêtre principale de l'application.....	39
--	----

I

Icône dans la zone de notification de la barre des tâches	37
INTERFACE DU LOGICIEL.....	37

K

Kaspersky Anti-Virus	
lancement au démarrage du système d'exploitation	96

L

Licence.....	188
active	188
Licence	
réception du fichier de licence	188

M

Menu contextuel	38
Mise à jour	
annulation de la dernière mise à jour	89
depuis un répertoire local.....	91
paramètres régionaux.....	90
source de mises à jour.....	89
utilisation du serveur proxy	90
Module d'analyse des liens	
Antivirus Internet	63

N

Niveau de protection	
Antivirus Courrier.....	53
Antivirus Fichiers.....	44
Antivirus Internet	61

O

Objet infecté	189
---------------------	-----

P

Performances de l'ordinateur	104
Planification	
mise à jour	92
recherche de virus	81

Q

Quarantaine.....	116
Quarantaine et Dossier de sauvegarde.....	116

R

Rapports	
enregistrement dans un fichier	131
filtrage.....	131
recherche d'événements.....	132
sélection du composant ou de la tâche.....	127
type d'événements	129
RAPPORTS.....	127
Réaction face à la menace	
Antivirus Courrier.....	54
Antivirus Fichiers	44
Antivirus Internet	61
recherche de virus	77
Recherche de Vulnérabilités	
compte utilisateur	85
liste des objets à analyser	84
planification	85
Réseau	
connexions sécurisées.....	110
Restauration	191
Restauration des paramètres par défaut	
Antivirus Courrier.....	58
Antivirus Fichiers	51
Restriction de l'accès à l'application.....	97

Z

Zone d'analyse	
Antivirus IM ("Chat")	67
Zone de confiance	
applications de confiance.....	106
règles d'exclusion	107
Zone de protection	
Antivirus Courrier.....	55
Antivirus Fichiers	45
Antivirus Internet	62